INTERNATIONAL JOURNAL OF SOFTWARE ENGINEERING & COMPUTER SYSTEMS (IJSECS)
ISSN: 2289-8522 e-ISSN: 2180-0650
VOL. 9, ISSUE 1, 27 – 38
DOI: https://doi.org/10.15282/ijsecs.9.1.2023.3.0107

ORIGINAL ARTICLE

Latest Advances on Security Architecture for 5G Technology and Services

K. O. Shobowale[1],*, Z. Mukhtar[2], B. Yahaya[2] ,Y. Ibrahim[2], M. O. Momoh[1]

[1]Department of Mechatronics Engineering, Airforce Institute of Technology Kaduna, Mando 800282, Kaduna, Nigeria.
[2]Department of Computer Engineering, Ahmadu Bello University, Zaria, 14330, Kaduna, Nigeria.

ABSTRACT – The roll out of the deployment of the 5G technology has been ongoing globally. The deployment of the technologies associated with 5G has seen mixed reaction as regards its prospects to improve communication services in all spares of life amid its security concerns. The security concerns of 5G network lies in its architecture and other technologies that optimize the performance of its architecture. There are many fractions of 5G security architecture in the literature, a holistic security architectural structure will go a long way in tackling the security challenges. In this paper, the review of the security challenges of the 5G technology based on its architecture is presented along with their proposed solutions. This review was carried out with some keywords relating to 5G securities and architecture; this was used to retrieve appropriate literature for fitness of purpose. The 5G security architectures are mojorly centered around the seven network security layers; thereby making each of the layers a source of security concern on the 5G network. Many of the 5G security challenges are related to authentication and authorization such as denial-of-service attacks, man in the middle attack and eavesdropping. Different methods both hardware (Unmanned Aerial Vehicles, field programmable logic arrays) and software (Artificial intelligence, Machine learning, Blockchain, Statistical Process Control) has been proposed for mitigating the threats. Other technologies applicable to 5G security concerns includes: Multi-radio access technology, smart-grid network and light fidelity. The implementation of these solutions should be reviewed on a timely basis because of the dynamic nature of threats which will greatly reduce the occurrence of security attacks on the 5G network.

ARTICLE HISTORY
Received: 12 June 2022
Revised: 7 November 2022
Accepted: 5 December 2022
Published: 1 January 2023

KEYWORDS
5G Technology
5G Mitigation
5G Network Treat
5G Security
5G Architecture

INTRODUCTION

The fact that 5G has the capability to create great economic values in all spares of life cannot be overemphasized. According to a report of the impact of 5G by the world economic forum in 2020 [1] , it is estimated that the global economic value due to the deployment of 5G will be around $13.2 trillion by the year 2035 which they predicted will pave the way for 22.3 million jobs for information technology discipline. Also, the rapid rate of devices and user equipment's that is being connected to this network is growing at an alarming rate. Connectivity is key in interfacing technological services such as the internet of things, artificial intelligence, robotics to name a few. With new technology comes new security threats that should be prevented with security solutions that will be able to overcome the existing and emerging security threats on the 5G network. Some of the 5G network security goals is to come up with techniques for security such as the segregation of suspicious traffic; communication security for the protection of sensitive data and information to ensure integrity and availability; access control for the authentication of users or machines on the network [2]; privacy protection among other security threats. One of the major security threats that can hamper the 5G network from intermitted down time is the authentication and authorization security threats [3] caused by Denial of service [4]. The frequency of this threats will reduce the economic value that can be accrued from the deployment of this technology. The existing authentication protocols for 5G networks are 5G-AKA (authentication and key agreement), EAP-TLS (extensible authentication protocol-transport layer security), and (extensible authentication protocol- authentication and key agreement) EAP-AKA [5]. Artificial intelligence algorithm based on machine learning and deep learning will help to automate threat/fraud detection and rectifying the network.

The fifth-generation technology of cellular network, 5G is a network system that uses new radio software (5G NR) as shown in Figure 1, with enhance capabilities of achieving high speed eMBB (enhanced mobile broadband), lower latency uRLLC (ultra-reliable low latency communication - less than one millisecond delay), multiple device connectivity and operation in higher frequencies mMTC (massive machine to machine type communication). The main difference with 4G and below with the 5G is the 5G New Radio, the new generation radio access network (NG-RAN) and the 5G core network. Deployment of 5G can make possible up to 10Gbps data transmission rates (about 10 to 100 times more than 4G and 4G-LTE) [1]. This technology will enhance and optimized the operation of other technologies (such as artificial intelligence, Internet of Things (IoT), cloud, big data and blockchain). Automated solutions are made easy with 5G due to the software nature of its deployment (through the technologies such as the software defined network (SDN), network function virtualization (NFV), Mobile cloud, cloud radio access network (C-

*CORRESPONDING AUTHOR | K.O. Shobowale | ✉ kshobowale@afit.edu.ng / kshobowale@gmail.com

RAN), network slicing (NS)) which makes it easy to process more real time data with less power. These qualities will make the development of several innovation possible which will drive economic development. The security of 5G is also dependent on the security of these aforementioned software technological solutions. 5G deployment is predicted to be the most important source of revenue in the future [6] as many industries operational processes such as manufacturing, construction, information and communication will be optimized which will consequently lead to more economic revenue generation.

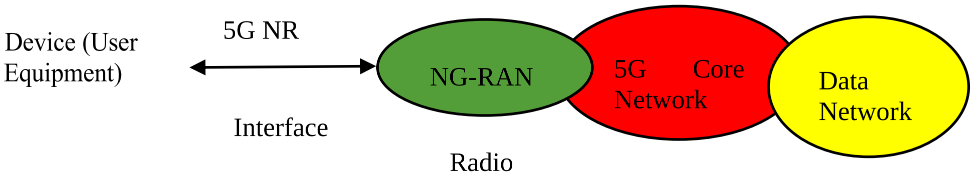

Figure 1. 5G System.

The role of digital economy in China after the pandemic was reported in [7] , it was reported that the digital economy powered by 5G accelerated economic activities during the peak of the pandemic and post pandemic. 5G network technology promotes economic growth. This will be hampered if the security of the network technology is hampered as there are vulnerable security concerns on the 5G network [8] [9], which can be obscure, persistent, complex and hard to detect as the architecture is a lot different from 4G due to the fact that it has quite a number of software-based architecture, thereby making it imperative for an overhaul of its security systems [10]. Part of the security concerns in 5G is to thwart threats from different attacks, malware and the use of intelligence in combating these threats [9]. It has also been reported that the existing security algorithms needs enhancement [11] in terms of robustness, automation, optimized flexibility that should be incorporated in the network architecture.

Most of the work on 5G security threats concentrate on one or a few technologies with limited number of threats and solutions. Therefore, this work is based on a broad category of 5G network security threats based on broad sources and architecture and proposed a wide range of solutions for mitigating the threats, taking into consideration the inherited security threats from the previous generations, security threats from extended architectures (such as IoT) and threats from new technologies (such as SDN, NFV, network slicing). In this work, emphasis is laid on 5G security based on its architecture which are the core network, the access network security (which includes the new radio), and the system security with a wide range of solution on how to mitigate these threats especially in areas such as authentication and authorization.

Our contributions are:

- A broad overview of the sources of security threats on the 5G network and mitigation plan for the threats.
- Discussed the hardware and software solutions to security threats on 5G network.
- Discussed the impact of different technologies in solving 5G security challenges.

This paper is organised as follows: section one depicts the overview of the 5G technology and its economic benefits. In section two, past research on the 5G network architecture, types of security threats and its applications are discussed. Section three reports the hardware and software solutions in relation to 5G security threats and the impact of different technologies while section four concludes with future directions.

RELATED WORK

The evolution of cellular network has followed a successive progression from the first generation 1G, second generation 2G, third generation 3G, fourth generation 4G and now the fifth generation 5G. The main objective of the succession is aimed at better and optimized network connectivity. The 5G is task with the goal of achieving high speed eMBB (enhanced mobile broadband), lower latency uRLLC (ultra-reliable low latency communication - less than one millisecond delay), multiple device connectivity and operation in higher frequencies mMTC (massive machine to machine type communication).

The impact of 5G on economic activities is basically on innovation and optimization of every facets of its existence, with innovation comes huge economical gains which can be achieved in areas that includes [1]: Optimized operational ecosystem; Intelligence which will lead to faster and effective processes; Better working environment (sustainability leading to optimized buildings/consumption, quality of life); Alleviates social issues that includes: traffic congestion, climate change, disaster safety. The immense economic benefits the deployment of 5G cellular network technology has on the economy are numerous as mentioned above, these benefits can be fully harnessed if efficient security protocols are put in place in every segment of the of the deployment to forestall potential security challenges that will threaten the 5G network and the users/devices on the network. It is worthy to note that because of the huge software architecture of 5G technology, the security protocol is diverse.

RESEARCH METHOD

A comprehensive literature review was conducted with the search words ‘5G security’, ‘5G architecture’, ‘5G technologies’, and ‘5G security mitigations’ from sources such as google scholar targeting reputable publications from sources such as web of science publication, scopus indexed journals, IEEE, elsevier journals as dipicted in Figure 2. A total of 150 publications was downloaded which was narrowed down to 56 articles based on their relevance to this topic. Each of the article is separated under its respective search keyword. The information pertaining to 5G security issues with respect to its architecture, technologies and mitigations was extracted to find patterns.

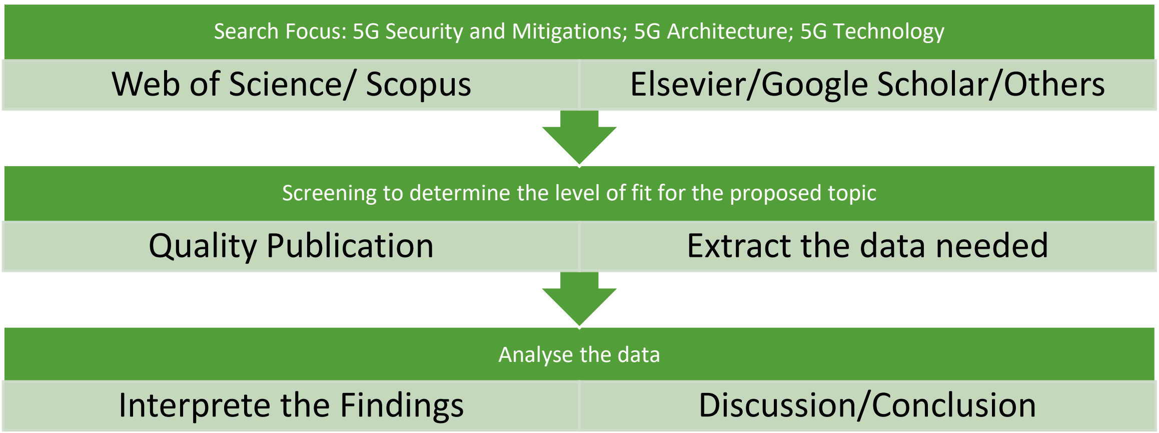
Search Focus: 5G Security and Mitigations; 5G Architecture; 5G Technology
Web of Science/ Scopus
Elsevier/Google Scholar/Others
Screening to determine the level of fit for the proposed topic
Quality Publication
Extract the data needed
Analyse the data
Interprete the Findings
Discussion/Conclusion

Figure 2. Research Methodology.

5G SECURITY ARCHITECTURE

The 3GPP (3G Partnership Project) body technical specification has highlighted sources of security concerns and key guides in the deployment of 5G technology which need to also be explored which are network access security, network domain security, user domain security, application domain security, service- based architecture domain security and visibility and configurability of security. The security concerns of 5G network were divided into different stages by [12 - 16]. In [12], it was divided into the user equipment (security issues pertaining to user equipment’s are: attack by mobile malware; 5G mobile botnets with actors Bot-master, Bot-proxy servers and Bots); access networks (security issues pertaining to access networks are attacks such as attack pertaining to false buffer status reports, message insertion); mobile operator core network (security concerns are attack on user data and identity privacy, radio resources and management attack, Distributed Denial of service, DDoS attack) and external internet protocol networks (could result in external network compromise). While in [13] , the four security concerns on a 5G network are denoted as authentication concerns, integrity concerns, privacy concerns and availability concerns. They recommended intrusion detection, cryptography and human measures as the mitigating measures for the security concerns. The network security architecture that was reported in [14] divided the 5G security network architecture into access network layer security, application layer security, management security, network security, user equipment security, virtualization and infrastructure security. They demonstrated the applicability of their security architecture with an IoT case study. 5G security threats was grouped into ten by [15] as SDN security, network slicing security, cloud radio access network (C-RAN) security, Edge security, software virtualization security, data security and privacy, open source/API security, supply chain security, predictive security/Monitoring and Analytics, and Optimization/Orchestration security. They discussed some of the security threats that can affect each of the 10 groups.

The work by [16] was closely related to the work of [13], their 5G security threat was based on Availability, Authentication, Confidentiality, Integrity and Non- Repudiation. They defined 5G availability as a function of radio access network, control plane and support system and that any attack on these systems impacts availability; while Authentication is a means to Non- Repudiation for device-to-device communication on the network. Integrity is applicable to user plane integrity protection and they reported that the radio access of the 5G works closely with cloud services whose security threats centres around Denial of service (DoS), this affects the operation of the network slice, jamming attack that impact the resources of the 5G radio access in [17], 5G security architecture was divided into Application layer security (such as smart grid, smart city, web application), service layer security (such as IoT, IoE), virtual layer security (virtual network, virtual compute), physical layer security (core network security), SDN security (data and control), Slicing security, Management and orchestration. They reported the architecture and challenges of 5G technology. The works in [18, 19, 20] also claasified 5G security based on some of the architecture and services that optimize the operation of the architecture. Sullivan et al., 2021[21] approach 5G security based on the OSI (Open Systems Interconnection) seven layer. They reported that the pysical layer security is the most vulnerable of the seven layer. Table 1 contains a summary of the recent 5G architecture and security threats reported in the literature.

Table 1. 5G Security Architecture and Threats.

Author	5G Security Architecture	Threat / Mitigations
Humayun et al., 2021 [5]	Security of radio interfaces	Jamming attack, Eavesdropping
	User plane integrity	DoS, DDoS, Eavesdropping, Jamming attack
	Access network layer security layer	Jamming attack, Eavesdropping, DoS, Flash network traffic, MiTM
	Roaming Security	DoS, jamming attack, Signalling storm
	5G infrastructure and End-user devices security	DoS, DDoS, Eavesdropping, MiTM
Mantas et al., 2015 [12]	User equipment	DoS attack, malware, MiTM, privacy leak
	Access networks	User equipment location tracking
	Mobile operator core network	DoS attack
	External internet protocol networks	DoS attack, malware
	Authentication concerns	Brute force attack
Ferrang et al., 2018 [13]	Integrity concerns	Cloning attack, message modification attack
	Privacy concerns	Eavesdropping, MiTM, spoofing,
	Availability concerns	Dos attack
Arfaouei et al., 2018 [14]	Access network layer security layer	Traffic spikes
	Application layer security	Authentication security threats
	Management security	Security control
	Network security	SDN security
	User equipment security	Privacy and data security
	Virtualization and infrastructure security.	DoS attack
Dutta&Hammad 2020 [15]	SDN security	DoS, API attack, MiTM, flooding
	Network slicing security	DoS, Side channel attack
	Cloud RAN security	DDoS, Intrusion attack
	Edge security	Cyber attack
	Software virtualization security	Hypervisor attack, Container attack
	Data security and privacy	Eavesdropping, Spoofing, Data manipulation
	Open source/API security	Data Manipulation
	Supply chain security	Malicious code injection attack
	Predictive Security/Monitoring and Analytics	Traffic attack
	Security in Optimization/Orchestration	Cache poisoning, Cache overwhelming
Park et al., 2021 [16]	Authentication	Control of knowledge / 5G AKA
	Availability	DoS, DDoS
	Confidentiality	Eavesdropping
	Integrity	Cloning
	Non-Repudiation	Data security
Ahmad 2017 [18]	Security in mobile cloud	XML DoS attack, malware
	Security in SDN	DoS attack, hijacking, MiTM attack
	Security in NFV	DoS attack, hijacking
	Security in Communication channel	IP layer attack, SDN scanner attack
	Privacy security	IMSI catching attack, timing attack, boundary
Hussain et al., 2019 [19]	Physical layer security	Jamming protection, bit encryption, spoofing
	Application layer security	Cryptographic mitigations

Sun et al., 2020 [20]	Network layer security	SDN/NFV network slicing control and automation
	Identity management	Authentication, key agreement, Authorization
	Security management	Security control, self-adaptive intelligence
	Identity management / Security Negotiation	Optimized user privacy, optimized control plane
	Application layer security	Authentication security threats
	Service layer security	DoS, DDoS, MiTM attacks
	Virtual layer security (SDN security, Slicing security, Management and Orchestration security)	Eavesdropping
	Physical layer security	Side-channel attack, Spoofing, data leakage / Encryption
Sullivan et al., 2021[21]	Physical layer security	Eavesdropping, Spoofing, Data manipulation / Beamforming, power control, Joint clustering
	Data link security	Rogue base station, Sybil attack, DDoS / Extensible authentication protocol
	Network security	DoS, MiTM, Eavesdropping, IP Spoofing, Packet Sniffing, Gateway attack
	Transport security	DoS, MiTM, Side Channel attack, Rule modification, Authentication. Authorization, Eavesdropping, Spoofing
	Session	DoS, MiTM, Authentication. Authorization, session restoration threats / Extensible authentication protocol
	Presentation security	Malicious data injection, format string
	Application security	Eavesdropping, information leakage, resource depletion, DoS, DDoS / Public Key Encryption, Lightning network and smart contract

Mitigations to 5G network security issues

The 5G internet of things (IoT) physical layer security was researched in [9], the task to be accomplished was divided into 4 sections, the first part was basically assessing common application possibilities of 5G IoT, followed by attacking 5G IoT physical layer using different scenarios, this was followed by analysing the opportunities and challenges of 5G IoT systems communication technologies and their ability to cope with threats at the physical layer, lastly, there was a discussion on research gaps and further research work with suggestion that more needs to be done to build algorithms that are resilience for 5G deployment. The author in [11], designed an algorithm for multiple input multiple output (MIMO) systems for 5G communications to assess the security level, they reported that the existing MIMO algorithms for assessment are not sufficient as there is still a considerable amount of noise at the physical layer of the security transmission. This they predicted could lead to possible eavesdropping of the network which could lead to compromise of the user's information. They used evidence base reasoning rules in their algorithm development which they reported gave an improvement on the existing algorithm and satisfactory results.. In the same line, [19] reviewed the 5G security in general and the security implication for an IoT based Vehicular Ad hoc NETwork (VANET) for implementation for commercial purpose. They reported that the VANET 5G security lies among 5G applications and business services, 5G core network, 5G cloud RAN, and connected users / devices. This makes them inherit the 5G security threats that are associated with these 5G technologies. New threats and security loop holes have been uncovered in networks including 5G, this makes assessment and evaluation of the 5G security to be checked from time to time to ascertain its capability to ward off emerging threats [17]. The work by [17] surveyed possible known and unknown threats that could affect 5G technology and suggested that more resilience is needed for security measures that will be appropriate for implementation in all aspects of the 5G technology. The work by [22] , reviewed the 3GPP 5G security concerns and discussed how they are applicable to IoT, Device-to-Device (D2D), Vehicle to everything (V2X), network slicing and access/handover. A review of 5G IoT security and privacy issues was reported in [23] with particular reference to access control, authentication, confidentiality, data integrity, key management, identity management, intrusion detection, policy enforcement, privacy, non- repudiation and trust. The work by Al-Turjman 2020 [29] was an extension of the security issues associated with one of 5G application area, 5G internet of nano- things (IoNT). They highlighted security issues in this respect into four groups which are: Local/global attack, Malicious/Rational attack, Active/Passive attack and Insider/Outsider attack. They further highlighted that these attacks can be intentional (attacks such as Dos, Malware and Man-in-the- Middle) and unintentional (attacks such as Black Hole and False information). Mitchell 2020 [31] also made recommendations on the measures to take to improve 5G security.

Security architecture of 5G C-RAN was classified into application domain security, network domain security network, access security and user domain security in [13], they reported that the separation of the data plane and the control plane resulted to a considerable security threats minimization. 5G cloud security and trust has been a source of issue and concern in its deployment as [19] reported that cloud access network (C- RAN) can suffer from threats such as single point of failure as the failure of the C-RAN will result in the whole network failure and consequently downtime, authorization issues, primary user emulation attack, and spectrum sensing data falsification. A design of a fibre network access trust- based blockchain authentication for software defined network was proposed in [24]. The proposed solution was designed to mitigate authentication security challenges with the users, equipment manufacturers, and the network operators. In solving the issue of eavesdropping that could result in privacy information leaks, [17] proposed channel quantization method to improve the security of C-RAN, in an environment with limited CSI. In [25], the security layer is proposed to be placed at the service plane (top most plane) to protect data and equipment from unauthorized access by ensuring authorized access control and identity recognition.

5G mobile cloud security concerns were reported in [18], the level of threat was categorized based on mobile cloud architecture as front-end threat, back-end threat and threat on the mobile network security. They also grouped security challenges into security in mobile cloud, security in software defined network (SDN), network function virtualization (NFV), communication channel security and privacy security while in [26], 5G security threats based on network architecture was explored. Table 2 summarizes the specific 5G security threats from the literature where the sources of threats and the resources that can be affected with the security concerns are reported. As an illustration, the 5G authentication security can affect the base station and user equipments which can lead to denial of service attack, eavesdropping among other authentication security concerns. Mitigations such as Blockchain technology has been deployed for authentication security [4].

Table 2. Specific 5G Security threats and mitigations from the literature.

Author	Area	Remark
Chow and Ma, 2021 [4]	5G authentication attack base station and user equipment with key emphasis on session key secrecy, device anonymity, mutual authentication, and	Proposed blockchain based protocol to mitigate DoS attacks, IMSI-catching, eavesdropping, replay attacks, man-in-the- middle attacks, backward secrecy and perfect session key forward
Zhang et al., 2021 [8]	Assessed 5G signaling interaction and its security mechanisms	Proposed Null security algorithm for mitigating 5G communication
Mantas et al., 2015 [12]	5G communication security	They prioritize the security of 5G on the user equipment, access networks, mobile operators core network and external internet protocol
Ferrag et al., 2018 [13]	Security threats in 5G network	They focused on authentication threat, integrity threat, privacy threat and availability threat
Arfaoui et al., 2018 [14]	Security architecture of 5G network	Focused on the 5G IoT and SDN security threats
Dutta and Hammad 2020 [15]	5G security challenges	They section the threats into 10 which includes cloud RAN security threat, Edge security threats
Ahmad 2017 [18]	5G cloud security	Focus on security challenges in SDN, NFV and cloud computing
Cao et al., 2019 [22]	3GPP Security threats in 5G network	Review of the 3GPP security concerns and some other security solutions for 5G use cases such as IoT and Device to Device (D2D)
Sicari et al., 2020 [23]	Security and privacy issues in 5G network	Focus was on 5G internet of things, fog computing and blockchain
Ahmad 2019 [26]	5G architectures that can be impacted by security threats	Focus on security challenges in network access, network domain, user domain, application domain, services domain, visibility and configurability
Saeed et al., 2021 [27]	Security issues in user privacy identity on the 5G network	Promotes the use of International Mobiles Subscribers Identifiers, short-term subscription identifier as Temporary Mobiles Subscribers Identifier, and Cell-Radio Networks Temporary Identifiers

Lv et al., 2021 [28]	Deep learning technology for mitigating 5G communication technology security challenges for the physical and network layer	The use of convolution neural network using unsupervised beamforming algorithm
Al-Turjman 2020 [29]	5G IoNT security threats	Focus on internet of Nano-Things
Yao et al., 2019 [30]	Security in 5G SDN	Simulation to test the Synchronized secret cryptographic authentication method proposed

According to [1] , the key technologies for 5G security are Security in massive MIMO (Multiple input multiple output), Security in SDN (Software defined networking), Security in NFV (Network function virtualization), security in UDN (Ultra-dense networking) and Security in Cloud Applications. 5G technical problems includes: Optimization (allocation problem), detection (minimized error rate), Channel Estimation problem. The work by Yao et al., 2019 [30] was on deploying a security solution in the software define network (application, data and control plane) which is to monitor and improve the performance of the network through software programming management and improve the network scalability. They proposed Synchronized secret cryptographic authentication for enhancing the security of the data and control layer of the software defined network of the 5G network. A review of the 5G security features with different cryptographic encryption algorithms was explored in [31], it was recommended that all security features on the 5G network should be deployed with 256-bit encryption keys.

SOFTWARE AND HARDWARE SOLUTIONS TO MITIGATE 5G SECURITY THREATS

Software implementation is built on hardware, as such highly scalable hardware security implementation is essential in the implementation of 5G as it is as important as software solutions. Trusted Platform module (TPM) is a type of hardware that enables scalable development of 5G trust edge computing nodes hardware security. Field programmable gate arrays (FPGA) was proposed by [32] as an hardware implementation for enhance security in 5G architecture. They listed areas where FPGA can be applied to 5G deployment as: in network slicing using network function visualization; cognitive radio, accelerator for cloud radio access network and massive multiple input multiple output characterization. Unmanned Aerial Vehicles which can act as an aerial base station, user equipment or communication relay was proposed by [2] for the prevention of security threats (Eavesdropping, spoofing and jamming) in 5G radio access network and services with mitigation spread to three zones (UAV secondary authorization, save zone and hot zone). For eavesdropping, sensors on the UAV were proposed to be used in monitoring the network and UAV relay can be used to create information communication safe zones. For spoofing, UAV can be use as the originator of secondary signal sources/enabler of secondary authorization with the capability to differentiate normal condition and spoofing attacks through modelling of the virtual channel while for jamming, multiple UAV, beamforming and dynamic relaying can be utilized to report hot zones. Software such as artificial intelligence (AI) has been reported to be promising in the mitigation of 5G security threats [3] [28]. AI was Proposed for authentication and authorization [3] , due to the fact that research directions are exploring the possibilities of alternative solutions to cryptographic solutions. AI can automatically combine and train important attributes/features for authentication and authorization to detect abnormal operations that can lead to security threats. A blockchain Federated learning model was proposed [33] to create smart contracts and mitigate the poisoning and membership inference attack security threats associated with deploring federated learning in 5G. Federated learning is a type of machine learning model where the training data is not required to be centralized, training can be run on participating host devices.

The role of artificial intelligence technologies in the of 5G security network solutions was presented in [28]. They apply deep learning convolution neural network with unsupervised beamforming algorithm to solving modulation information challenges in the physical layer communication technology which they reported outperformed the traditional algorithms. The moving target Défense (MTD) concept involves: virtual machine migration, shuffling of internet protocol address, network/software resources replication and diversifying network path; this can be used to induce resilience in 5G network security with the aid of 5G technologies such as SDN and NFV [3]). In mitigating the denial-of-service attack, the research by [4] [34] explore different methods. Chow and Ma, 2021 [4] worked on base station and user equipment authentication whose protocol is based on blockchain and key agreement on the 5G network. They reported that with their implementation, they were able to achieve device anonymity, mutual authentication, perfect forward secrecy, resistance to DoS attacks and key agreement while Singh et al, 2022 [34] proposed the use of statistical process control for jamming attack detection which was applied to opportunistic wireless networks. They reported that other methods that can be used includes: Markov chain models, trust base, game theory and auto regression. INSPIRE-5G plus was developed by [35] as a 5G security platform incorporating technologies such as artificial intelligence and blockchain.

5G SECURITY CONCERN MITIGATIONS AND OTHER TECHNOLOGIES

In other to mitigate 5G security concerns, the architecture and the services that makes up the technology has to be studied for probable security aspects to take into consideration. Authentication, Availability, Integrity, Non-repudiation, and confidentiality are 5G security aspects that has been widely reported in the literature. The software defined network controller (SDNC) and its vulnerabilities that could impact its normal operation includes: Impersonation, spoofing, DDoS, MiTM attack, API flood attack. The 5G network is being controlled by the SDNC and it is software base which makes it the manager of the traffic flow and policies on the network, any security threat can make the entire network fail [35]. They also reported that the DDoS attack is one of the dangerous attacks on the SDNC, therefore to mitigate DDoS attack detection, Ramamurthy, 2019 [36]and Tan et al., 2020 [37] implemented a machine learning algorithm. In Ramamurthy, 2019 [36] support vector machine (SVM) was used while in Tan et al., 2020 [37], a combination of K-Means and KNN machine learning algorithm was used. Gadze et al., 2021 [38] implemented a deep learning algorithm (long-short term memory and convolutional neural network). Network Slices are partitioned multiple virtual networks that serves the purpose of fulfilling all the required services that are demanded on the 5G network by keeping each service in their respective slice; partition. The security vulnerabilities that are peculiar to network slicing which includes that of the software defined network (SDN), network function virtualization (NFV) and cloud radio access network (C-RAN). Its security is based on all the processes involved in its lifecycle. Dangi et al., 2022 [39] reported a review on network slicing mitigation based on machine learning in the areas of its life cycle which are: planning and design (support vector machine SVM, Decision tree, Gradient decision tree, spectral clustering, reinforcement learning), security (Deep neural network DNN, principal component analysis PCA), monitoring (DNN, PCA, k-means clustering, spectral clustering), operations and management (DNN, reinforcement learning, k-means clustering), and fault detection (PCA, logistic regression, Bayesian network, independent component analysis) which has the key elements: security, slice classification, resource allocation, slice allocation, slice admission, and network load balancing. They subdivided areas of network slices as 3 which are the core network slicing, radio access network slicing and end to end slicing. They reported a list of machine learning and deep learning algorithms that has been applied to network slicing security such as SVM, KNN, random forest, decision tree, deep reinforcement learning. The authentication security concerns with the most common attacks are MiTM attack, impersonation, temporary information disclosure attack. Cryptography has been widely used in this types of attack, and research works are looking at the use of solutions such as artificial intelligence and blockchain.

The 5G security threats has been grouped into 3 which are the access network security, the core network security and the system security to encompass all the other infrastructure and user equipment security threats as contained in Table 3 together with their suggested solutions. For instance, the radio access key interface security concerns of the access network can be solved by using the host identity protocol. In Table 4, other 5G security services threats such as wireless fidelity (Wi-Fi), light fidelity (Li-Fi), mobile cloud, multi-access edge computing (MEC) and IoT are presented. For MEC cloud, Ding 2020 [40] grouped sources of security threats into 5 as shown in Table 4, while [33] proposed federated learning and blockchain smart contract to mitigate security concerns in MEC. Also, solution that has been proposed for MEC infrastructure mitigations includes: Multi-radio access technology, smart-grid network [42]. Li-Fi has been reported to give security to 5G network on applications areas such as IoT, high speed wireless connectivity, and smart home/ road/ health deployments [43-44] while Intrusion detection techniques was covered in [45]. The deployment of IoT on 5G network is also prone to security threats such as: IoT application network protocol layer on the architecture of the 5G, connected devices and the internet service application servers [46]. It was also reported that technologies such as software defined network, network function virtualization, network slicing and information centric networking will afford a formidable security architecture for better security implementation [40]. Artificial intelligence has found its way in 5G security issues in different capacities, in the mitigating 5G security, machine learning has been used to design, model and automate security ptotocols [47]; for intelligent and secure drone communication [48], they used AI and blockchain and divided the implementation into the application layer, the UAV layer, edge-AI layer, blockchain layer and the communication layer. AI was used for multilayer intrusion detection for SDN and NFV in five layers which are the virtualization layer, data acquisition layer, domain controller layer, smart controller layer and the switches layer [49]. 5G network automation prompted the implementation of AI in [50] while the level of adoption of AI and machine learning for data analytics, control and automation in respect of supervised learning, unsupervised learning and reinforcement learning was highlighted in [51].

Table 3. 5G Security layer, threats, needs and mitigations.

Architecture	Type	Security threats and suggested solutions	Security needs and suggested solutions
Access Network Security	i. Radio Access Network and their interfaces Security (combinations of different access technologies) i.e cellular Network RAN (having Base stations, Wifi, LiFi and so on). ii. Design Optimized key management protocol.	i. Radio interface key **with:** Host identity protocol [10]. ii. Jamming attacks of the radio signals and channels **with:** Random key distribution Spread spectrum technique [5]. iii. Small cell nodes security iv. DoS attacks	i. Integrity protection ii. Confidentiality
Core Network Security	i. Control of Network (by operator and vendor). ii. Network Function Virtualization (NFV) – (Virtual Network Functions, VNF) for cloud or server deployment. iii. Software Defined Network (SDN) – (application layer, controller layer, infrastructure layer) **with:** Synchronized secret cryptographic authentication [4].	i. Signalling-based threats DoS/DDoS attack **with:** DNS protection, Network monitoring, anti-DDoS hardware [53]. ii. Spoofing attack / Replay attack Eavesdropping **with:** Network access control, Encryption, physical security, Network segmentation, PLS analysis [52] iii. Hijacking iv. Resource exhaustion attack v. MiTM **with:** Data encryption, manual authentication, Intrusion Detection System [56]	i. Network domain security ii. NFV (Integrity, Authenticity, iii. Confidentiality, Non-repudiation) **with:** Encryption Subscriber privacy (from identity, location, data) with: dynamic credential generation; in- device spatial cloaking; anonymous authentication; artificial noise; MobiCloud [27][56] iv. Subscriber authentication v. Network Slicing / Isolation (with SDN, NFV, C-RAN) **with:** Slice categorization, slice isolation, intrusion detection system [15]. vi. Trust issues
System Security	On network infrastructure, user equipment	i. DoS / DDoS Attack ii. Int. mobile subscriber identity catching attack iii. Advance malware iv. IoT botnets v. Device tampering vi. Hacking firmware vii. User identity theft viii. Spyware	i. Authentication **with:** 5G AKA, EAP TLS, EAP AKA, Machine Learning [4]. ii. Integrity of the user plane (data manipulation, code injection) **with:** end to end encryption, Blockchain access control [4] iii. Availability **with:** Pseudorandom time-hopping spread spectrum, optimized resource allocation, centralized security system [54] iv. Upgrades v. Orchestration vi. Access and key management of security data **with:** Low-Density Parity-check codes, Lattice codes, polar codes, PLS [54]. ●Monitoring ●Signalling storm **with:** C-RAN, Edge computing ●Roaming security **with:** SDN

Table 4. 5G Services Security.

5G Services	Types	Threats
5G WiFi security	Mac Layer, Network layer, transport layer, application layer	Flaws in network security DoS attack **with:** Statistical process control [41]. Direct-sequence spread spectrum, Frequency-hoping spread spectrum Impersonation attack Confidentiality attacks Anonymity gains
5G LiFi security	Protection of data integrity Privacy of mobile users	DoS threat User confidentiality threat Gateway's impersonation Flaws in authentication network security Access gains by end user anonymity
Mobile cloud security	Front-end	Physical **with:** Massive MIMO, Millimeter wave Application (i.e Malware) **with:** Anti-malware; elastic applications
	Back-end	Cloud servers **with**: Intrusion detection [45] Virtual machines Data storage Systems Protocol Hypervisor
	Mobile network i. Radio access network (i.e Wi-Fi) **with:** C-RAN ii. Cloud radio access network iii. Virtualization security iv. Cyber-physical system security v.Secure and private data computation vi. Cloud intrusion vii. Access control	Wi-Fi sniffing DoS Session hijacking Address impersonation, MiTM
Multi-access Edge Computing (MEC) Security threats in 5G **with:** Federated learning and blockchain smart contract [33]	Network Infrastructure Core Servers Edge Servers Virtualization End devices	DoS, MiTM, Rogue mobile router Privacy issues, service manipulation, Rogue core server, Privacy issues, Equipment damage, service manipulation, Rogue mobile server DoS, Privacy issues Service manipulation of the virtual machine, Data injection
IoT Security	Dynamic address/ID shuffling strategy 5G network infrastructure[46] Devices on the network Internet service application servers	DoS/DDoS attacks, Impersonation jamming attacks eavesdropping

CONCLUSION

The information in the literature is diverse and the understanding of the main security challenges that are associated with the deployment of 5G technology are becoming apparent as the technology is deployed and real-life use cases are tested. The bodies overseeing the regulation and standardization of the 5G network has security specifications which have generally different presentation from the literature. From the architecture of 5G technology, it is apparent that different parties manage their own part on the 5G network which makes trust a key security concern, together with the associated standardization, regulation and dynamic security issues. All threat levels based on the architecture and its associated services should be taken into consideration to achieve the best security policies for this technology. The most prominent security threats are found in the architecture and its surrounding services and the most apparent security attacks includes: Denial of service attack, malware, Man-in-the-Middle attack. Hardware and software security implementation has been discussed together with some mitigation techniques.

The 5G security architecture basically are in the OSI (Open Systems Interconnection) seven layer of the network. Understanding the complete architecture of this network security as regards the 5G technology is a first step towards the mitigation of security threats on the 5G network. The 5G security concerns lies in the 5G core network, 5G cloud RAN, 5G data network and connected users / devices together with all their associated technologies that they are all connected with. Majority of the 5G security challenges are related to authentication and authorization such as denial-of-service attacks, man in the middle attack and eavesdropping on the network.The software solutions that have been proposed includes: artificial intelligence (machine learning algorithm such as: support vector machine (SVM), K-Means and KNN; deep learning algorithm (such as long-short term memory and convolutional neural network), Blockchain and Statistical Process Control while the hardware solutions includes: Trusted Platform module (TPM), Field programmable gate arrays (FPGA), Unmanned Aerial Vehicles. Other technologies that have also been reported to be effective are Multi-radio access technology and smart-grid network on the MEC and light fidelity (Li-Fi) for 5G IoT.

The continual joint efforts by all parties in the fight against security threats will ensure the services and economic values that is associated with the deployment of the 5G technology can be achieved. For future research, each of the architecture and services will be evaluated in-depth for better understanding of the causes and effects it has on performance of the 5G system and its effect on the economy. Also, the analysis of the software aspect of 5G technology will be undertaken.

ACKNOWLEDGEMENT

The authors would like to thank all the anonymous reviewer for their invaluable contributions.

REFERENCES

[1] The impact of 5G: Creating new value across industries and society (2020, January). Retrieved February 5, 2022, from: https://wwww.weforum.org/whitepapers.

[2] A.S. Abdalla, K. Powell, V. Marojevic and G. Geraci, "UAV-assisted attack prevention, detection, and recovery of 5G Networks," *IEEE wireless comm.,* 2020.

[3] C. Benzaid and T. Taleb, "AI for beyond 5G Networks: a cyber-secuirty Defense or offence Enabler," *IEEE network,* 2020.

[4] M.C. Chow and M. Ma, "A blockchain- enabled 5G authentication scheme against DoS Attacks," *Journal of Physics: Conf. Series,* 2022.

[5] M. Humayun, B. Hamid, N. Jhanjhi, G. Suseendran and M. N. Talib., "5G Network Security Issues, Challenges, Opportunities and Future Directions: A Survey," *Journal of Physics: Conf. Series,* 2021.

[6] M. Z. Noohani and K. U. Magsi, "A Review of 5G Technology: Architecture, Security and wide Applications," *Int Research Journal of Eng. and Tech.,* vol. 7, no. 5, 2020.

[7] X. Jiang, "Digital economy in the post-pandemic era," *Journal Of Chinese Economic and Business Studies,* vol. 18, no. 4, p. 333–339, 2020.

[8] R. Zhang, W. Zhou and H. Hu, "Towards 5G Security Analysis against Null Security Algorithms Used in Normal Communication," *Hindawi Security and Comm. Networks*, 2021.

[9] P. P. Sriram, H.-C. Wang, H. G. Jami and K. Srinivasan, "5G Security: Concepts and Challenges," *Springer Nature Switzerland,"* 2019.

[10] M. Liyanage, I. Ahmad, A. B. Abro and A. G. a. M. Ylianttila., "A comprehensive guide to 5G Security," John Wiley and Sons, 2018.

[11] S. Yan, D. Yin, X. Song, X. Dong, G. Manogaran and G. Mastorakis, "Security situation assessment for massive MIMO systems for 5G Communications," *Future Generation Comp. Sys,*" p. 25–34, 2019.

[12] G. Mantas, N. Komninos, J. Rodriuez, E. Logota, H. and Marques, (2015). "Security for 5G Communications," In: Rodriguez, J. (Ed.), Fundamentals of 5G Mobile Networks. (pp. 207-220). John Wiley & Sons, Ltd.

[13] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Comp. Applications,* pp. 55-82, 2018.

[14] G. Arfaoui et. al, "A Security Architecture for 5G Networks," *IEEE Access,* 2018.

[15] A. Dutta and E. Hammad., "5G Security Challenges and Opportunities: A system approach," *IEEE Xplore*, 2020.

[16] J. H. Park, S. Rathore, S. K. Singh, M. M. Salim, A. E. Azzaoui, T. W. Kim, Y. Pan and J. H. Par, "A Comprehensive Survey on Core Technologies and Services for 5G Security: Taxonomies, Issues, and Solutions," *Human-centric computing and info. sci*, 2021.

[17] D. Xu, P. Ren, Q. Du, L. Sun and Y. Wang, "Towards win-win: weighted-voronoi-diagram based channel quantization for security enhancement in downlink cloud-ran with limited csi feedback," *Sci. China Inf. Sci.,* 2017.

[18] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov "5G Security: Analysis of Threats and Solution " *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*

[19] M. F. Hossain, A. U. Mahin, T. Debnath, F. B. Mosharrof and K. Z. Islam., "Recent research in cloud radio access network (C-RAN) for 5G cellular systems - A survey," *Journal of Network and Computer Applications*, p. 31–48, 2019.

[20] Y. Sun, Z. Tian, M. Li, C. Zhu, N. Guizani, "Automated attack and defence framework towards 5G security," *IEEE Network ,* 2020.

[21] S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, "5G Security Challenges and Solutions:A Review by OSI Layers" IEEE Access, vol. 9, 2021.

[22] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu and Lihui Xiong, "A Survey on Security Aspects for 3GPP 5G Networks," *IEEE Comms Surveys & Tutorials,* 2019.

[23] S. Sicari, A. Rizzardi and A. Coen-Porisini, "5G In the internet of things era: An overview on security and privacy challenges," *Computer Networks,*179, 2020.

[24] H. Yang, Z. H. J. Zhang, Y. Wu, Y. Lee and Y. Ji, "Blockchain-based trusted quthentication in cloud radio over fiber network for 5G," *international conference on optical communications and networks (ICON),* pp. 1-3, 2017.

[25] J. Wu, Z. Zhang, Y. Hong, Y. Wen "Cloud radio access network (C-RAN): a primer.," *IEEE Network*, vol. 29, no. 1, p. 35–41, 2015.

[26] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, M. Ylianttila, *IEEE Comms. Surveys & Tutorial*, 2019

[27] M.M. Saeed, M.K. Hasan, A.J. Obaid, R.A. Saeed, R.A. Mokhtar, E.S. Ali, Md Akhtaruzzaman, S. Amanlou, A.K.M. Zakir Hossain, "A comprehensive review on the users' identity privacy for 5G networks," *IET Communications*, 2021.

[28] Z. Lv, A. K. Singh and JinhuaLi, " Deep Learning for Security Problems in 5G Heterogeneous Networks," *IEEE Network*, 2021.

[29] F. Al-Turjman, "Intelligence and security in big 5G-oriented IoNT: An overview", Future Generation Computer Systems, p. 357–368, 2020.

[30] J. Yao, Z. Han, M. Sohail and Liangmin Wang, " A Robust Security Architecture for SDN-Based 5G Networks," *Future Internet*, 2019.

[31] C. J. Mitchell, "The impact of quantum computing on real-world security: A 5G case study," *Computers & Security*, p. 93, 2020.

[32] V. Chamola, S. Patra, N. Kumar, and M. Guisani, "FPGA for Re-configurable Hardware for Next Generation Communication, " *IEEE Wireless Comms.*, 2020.

[33] Y. Liu, J. Peng, J. Kang, A. M. Iliyasu, D. Niyato and A. A. A. El-Latif, "A Secure Federated Learning Framework for 5G Networks," *IEEE Wireless Comms*, 2020.

[34] Z. Lv, A. K. Singh and JinhuaLi, "Deep Learning for Security Problems in 5G Heterogeneous Networks," *IEEE Network*, 2021.

[35] J. O. Ramon et al., "INSPIRE-5Gplus: Intelligent Security and Pervasive Trust for 5G and Beyond Networks" *ARES* 2020, August 25–28, 2020, Virtual Event, Ireland

[36] S. Y. Mehr and B. Ramamurthy, " An SVM based DDoS attack detection method for Ryu SDN controller," *Proceedings of the 15th Int. Conf. on emerging networking experiments and technologies*, 2019.

[37] L. Tan, Y. Pan, J. Wu, J. Zhou, H. Jiang and Y. Deng., "A new framework for DDos attack detection and defence in SDN environment.," *IEEE Access 8*, 2020.

[38] J.D. Gadze, J.O. Agyemang, A.A. Banfo-Asante, H. Nunoo-Mensah and K. A-B. Opare, "An investigation into the application of Deep Learning in the Detection and Mitigation of DDOS Attack on SDN Controllers," *Technologies*, vol. 9, no. 14, 2012

[39] R. Dangi, A. Jadhav, G. Choudhary, N. Dragoni, M.K. Mishra and P. Lalwani "ML-Based 5G Network Slicing Security: A Comprehensive Survey" *Future Internet*, vol. 14, no. 116, 2022.

[40] A.Y. Ding*, "*MEC and Cloud Security*, " Wiley 5G Ref, p. 1–16, 2020.*

[41] J. Singh, I. Wounganag, S.K. Dhurandher, K. Khalid "A jamming attack detection technique for opportunistic network" *Internet of Things*, vol. 17, 2022.

[42] P. Panaweera, A. Jarcut, M. Liyanage " MEC- enabled 5G use cases: A survey on security vunerabilities and countermeasures" *ACM Computing Surveys*, vol. 54, no. 9, 2021.

[43] H. Haas " LiFi is a paradigm-shifting 5G technology" *Reviews in Physics*, vol 3, p. 26–31, 2018.

[44] G. Albert, G. Dekel, S. Kurland, M. Ran, D. Malka, G. Katz, "Which LiFi's apps may fit mostly to 5G and beyond- 5G Technology?," *2019 Global LIFI Congress (GLC)*.

[45] K. Gai, M. Qiu, L. Tao, Y. Zhu, "Intrusion detection techniques for mobile cloud computing in heterogenous 5G" *Security Comm. Networks*, vol. 9, p. 3049-3058, 2016.

[46] H. Kim "5G core network security issues and attack classification from network protocol perspective" *Journal of Internet Services and Information Security (JISIS)*, vol 10, no. 2, p. 1-15, 2020.

[47] A. Afaq, N. Haider, M.Z. Baig, K.S. Khan, M. Imran, I. Razzak "Machine learning for 5G security: Architecture, recent advances, and challenges" *Ad Hoc Networks*, 123, 2021.

[48] R. Gupta, A. Kumari, and S. Tanwar, "Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications," *Transactions on Emerging Telecomms Technologies*, 2020.

[49] I. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz, S. M. A. Akber, "Multi-layered Intrusion Detection and Prevention in the SDN/NFV Enabled Cloud of 5G Networks using AI-based Defense Mechanisms," *Computer Networks*, 2020

[50] O. Hireche, C. Benzaïd,T. Taleb "Deep data plane programming and AI for zero-trust self-driven networking in beyond 5G," *Computer Networks* 203, 2022.

[51] M. Usama, I. Ilahi, J. Qadir, R. N. Mitra and M. K. Marina, "Examining Machine Learning for 5G and Beyond Through an Adversarial Lens," *IEEE Internet Computing*, vol. 25, no. 2, p. 26–34, 2021.

[52] L. Sun, K. Tourki, Y. Hou, L. Wei "Safeguarding 5G Networks through Physical Layer Security Technologies", *Wireless Comms. and Mobile Computing*, 2018.

[53] S. Köksal, Y. Dalveren, B. Maiga, and A. Kara, "Distributed denial-of-service attack mitigation in network functions virtualization-based 5G networks using management and orchestration" *Int. Journal of Comm. Sys*, vol. 34, no 9, 2021.

[54] D. Fang, Y. Qian, and R. Q. Hu "Security for 5G Mobile Wireless Networks" *IEEE Access*, 2017

[55] H. Yi, "Improving security of 5G networks with multiplicative masking method for LDPC codes," *Comps and Electrical Engrg*, 95, 2021.

[56] F. Liu, L. Su, B. Yang, H. Du, M. Qi, and S. He, "Security Enhancements to Subscriber Privacy Protection Scheme in 5G Systems," 2021 *Int. Wireless Comms and Mobile Computing Conf (IWCMC).*