IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Review Paper On Comprehensive Study Of Application Of Networking In Different Domain

Nikunj Patel[1], Himanshu Soni[2], Mrs. Nisha Rathore[3]

1) Student BCA 3rd Semester, Amity University, Chhattisgarh,

2) Student BCA 3rd Semester, Amity University, Chhattisgarh,

3)Assistant Professor, ASET, Amity University, Chhattisgarh,

Abstract—This comprehensive survey delves into the complex landscape of modern information and communication technologies, including cloud computing, the Internet of Things (IoT), software-defined networking (SDN), artificial intelligence (AI), and emerging technologies such as: We are investigating various fields such as. Blockchain service (BaaS). This story unfolds against the backdrop of continuous technological advances and highlights the central role of network technologies in reshaping computing and communications. This study traces the history of computer networking from its beginnings in the ARPANET to the commercialization of the Internet, navigating key developments such as the rise of TCP/IP and the transformative era of cloud computing and his IoT. It carefully examines the challenges and advances inherent in this digital environment and reveals the important interactions of network technologies in different fields. Future Scope describes promising research directions such as cloud security, IoT vulnerabilities, SDN optimization, and integration of new technologies such as blockchain. The focus is on improving security measures, addressing network challenges, and maximizing the potential of AI and cognitive computing in diverse business environments. The study envisions a future where evolving technologies contribute to a more connected, secure and efficient digital environment, and calls on researchers to prioritize innovation, efficiency and security across a range of sectors. Essentially, research environments must be rooted in a commitment to a future of digital transformation that aligns with the needs of connectivity, security, and innovation.

Keywords— cloud security, Internet of Things, network security, Network Functions Virtualization, Secure Socket Layer, Distributed Denial of Service attacks, 5G wireless backhaul networks, Blockchain as a Service, Cloud Radio Access Network, traffic engineering.

I. INTRODUCTION

In a period characterized by tenacious innovative advancement, the significant effect of organizing ranges a heap of spaces, revolutionizing the scene of data handling and communication. This survey paper fastidiously navigates through a differing range of basic subjects, extending from the complexities of cloud security and the broad domain of the Internet of Things IoT to the transformative impact of Software Defined Organizing SDN, encryption techniques, Organize Capacities Virtualization NFV, and the combination of unmistakable light communication with situating advances inside the setting of 5G systems. In the midst of the heap benefits

advertised by cloud computing frameworks, the paper underscores the basic for strong security measures, both specialized and organizational, to brace delicate information handled inside these energetic situations. As mechanical strides usher in phenomenal capabilities, the paper comprehensively investigates the challenges and headways inborn in this computerized scene, shedding light on the basic part played by organizing innovations over multifaceted spaces.

II. BACKGROUND & HISTORY

The advancement of organizing advances has navigated a energetic scene, ceaselessly moulded by the tireless interest of network and data trade. The roots of advanced organizing follow back to the early days of computer organizing, eminently stamped by the improvement of ARPANET within the late 1960s, conceived by the Joined together States Division of Defences Progressed Inquire about Ventures Office ARPA. This spearheading exertion laid the foundation for bundle exchanging, a principal concept in information communication. The ensuing decades seen the multiplication of organizing conventions and models, with the rise of TCP IP as a urgent standard that supports the worldwide web. The 1990s saw the commercialization of the Web, catalysing a progressive move in how people and organizations gotten to and shared information. As computing control surged and advancements burgeoned, the 21st century introduced in a period of phenomenal network. Cloud computing risen as a transformative worldview, empowering adaptable and on demand get to computing assets. At the same time, the Web of Things IoT burgeoned, interconnection gadgets and empowering the consistent trade of data. The rise of Software-Defined Organizing SDN and Organize Capacities Virtualization NFV encourage stamped a take-off from conventional organizing structures, presenting programmability and adaptability. In the midst of these propels, the tireless challenges of security, protection, and the optimization of organize execution have become central focuses within the continuous story of organizing advancement. Nowadays, the crossing point of developing advances, from 5G systems to Blockchain, proceeds to redefine the boundaries of what is achievable within the interconnected world.

III. BACK PAPER REVIEW OR PAST RESEARCH WORK

The International Journal of Research Publication and Reviews presents a paradigm for managing and safeguarding private information in cloud computing settings [11]. Three tiers of data classification, cloud abuse prevention, and encryption are covered in this study. To reduce data security breaches, cloud platforms that handle sensitive data must put in place organisational and technical security safeguards. A few of the many benefits that cloud computing systems have over conventional data processing techniques include the automated tools that allow virtualized resources to be created, connected, configured, and reconfigured whenever needed. But as cloud computing has become more widely used, security and privacy issues about its features—like multi-tenancy, trust, loss of control, and accountability—have quickly surfaced due to this paradigm change. 76% of businesses will use Amazon Web Server (AWS) by 2020, and 63% will use Microsoft Azure.

The research paper titled “The future of IOT and biometrics” [18]. The networking of different everyday objects using wireless, mobile, RFID, and sensor technologies is known as the Internet of Things (LoT). Researchers and users are concerned about LoT security because of the vulnerabilities in ports on objects, connected devices, and networks. Proper security and privacy are essential for the LoT business model to work. The LoT secure approach, which makes advantage of end-user and user bluemetric capabilities, is explained in this chapter. The article discusses five different kinds of assaults, such as data and identity theft, man-in-the-middle attacks, and botnets, that affect LoT Internet-powered systems. The goal of identity theft is to gather information that can identify a lot about an individual.

In order to address the shortcomings of conventional network topologies, Software-Defined Networking, or SDN, is being referred to in this article as an emerging network architecture [17]. By introducing a decoupled architecture, SDN makes it simpler to design, administer, and troubleshoot networks and permits customisation within them. Aspects of network architecture such as design, programmability, security, security behaviour, and vulnerabilities are covered in this text. Furthermore, in order to further determine the impact of the attack and offer mitigation techniques, a variety of architectural vulnerabilities are examined, and attack routes are further created at each level. The Creative Commons Attribution Licence is used to disseminate this open access publication.

This article is a review article on network security and encryption in computer science and technology [16]. This document provides an overview of network security and describes various techniques to improve network security, including encryption. Cryptography is the science of writing secret code and involves creating and analyzing protocols that block attackers. It is important to ensure that data confidentiality, integrity, authentication, and non-repudiation are at the heart of modern encryption. This article also discusses testing issues for successful exchange of encrypted information and secure exchange of keys between sender and receiver. It points out that information security and information security should be ensured to the extent that specialized distributed storage organizations cannot decrypt the information. Additionally, information must first be encrypted by the customer before being offloaded to a distributed, remote storage location.

The research paper titled “Network Functions Virtualization” [15], A developing technique called network functions virtualization (NFV) uses virtualization technology to isolate the software implementation of network services from the underlying hardware. Network function virtualization (NFV) speeds up new service launches and enhances network service delivery. But there are also difficulties, such making sure virtual appliances operate on networks, dynamic instantiation and migration, and effective deployment. This article addresses the obstacles and potential paths for this field of study while giving a quick summary of NFV, its specifications, and its architectural framework. Firewalls, DPI, NAT, VPNs, CDNs, routers, packet, data network gateways, and IP Multimedia Subsystems (IMS) are examples of common NFV-based approaches to network devices. Network carriers may gain from NFV in a number of ways, including lower energy and capital expenditure costs and faster delivery of customised and targeted services.

The research paper titled “Artificial intelligence and Cognitive computing” [14], The application of partial least squares to structural equation modelling for AI and cognitive computing data analysis is covered in this article. The Paper highlights how well these technologies function in a commercial setting and highlight the features that businesses find most intriguing. The advantages and disadvantages of each technology are also covered in this article, depending on the activity or business that your organisation is attempting to optimise. It underlines how crucial it is to identify the differences between CC and AI's capabilities in order to optimise their respective advantages. The Creative Commons Attribution Licence is used to disseminate this open access publication.

In the article, Christian Johan Lamprecht investigates the viability of the Secure Socket Layer (SSL/TLS) protocol's trade-off between runtime security and performance. The writers create adaptive security methods that enhance non-adaptive legacy security systems with adaptive features. To produce a workable version of Adaptive SSL (ASSL) solution, this methodology is applied to the SSL protocol. By efficiently fine-tuning security at runtime, this method can lower the maximum server load by as little as 15% or even more, depending on how sophisticated the tuning choice is. Paper have effectively shown that the key components of this methodology's implementation are an infringement policy and ASSL. .In addition to discussing the necessity of data integration, reaction time, and maintenance research, the essay highlights the significance of human-centered information communications in cloud networks. It presents a selection of research articles on subjects like hybrid vulnerability analysis, distributed data management, and hybrid networking systems. In order to guarantee excellent accuracy and enhance the search, the study suggests a probabilistic strategy based on the Basic Local Alignment Search Tool (BLAST). The shortest-path problem with precedence constraints of increasing complexities is solved by developing an improved order-based genetic algorithm in

this paper, which focuses on the speed of high-performance bioinformatics. Additionally, it suggests a customized user experience paradigm to enhance cognitive risk assessment and detection.

The research paper titled “Adaptive Security” [13], The CyberSec4Europe project aims to develop flexible security solutions that can adapt to changes in security. We provide tools and techniques to support the detection and mapping of assets, security requirements, and threats in a variety of areas. This project was funded by the European Union's Horizon 2020 program under funding agreement. This paper provides an analysis of key research questions regarding adaptive security and identifies trends, patterns, and gaps in existing research. This study asks three types of research questions related to the role of application domains, stakeholders, and requirements in adaptive security. The information contained in this document is provided as is, without warranty or implied warranty of its suitability for any particular purpose.

The integration of location and visible light communication into 5G networks for the Internet of Things (IoT) is covered in this article [12]. This highlights the requirement for fast data speeds, high positioning precision, low latency, low battery consumption, and enhanced security for IoT devices. To meet these needs, this article presents a multilayer network architecture that combines VLC and VLP. The optical atcell layer offers high speed transmission and precise positioning services, while the macrocell and picocell levels support greater coverage and reliability across the radio frequency (RF) spectrum. Technologies like as modulation, energy harvesting, and various access techniques are essential for enhancing performance. Case studies and simulation analysis are used to illustrate the merits and benefits of the suggested multi-layer network for IoT.

The history, motivations, and classification of Distributed Denial of Service (DDoS) assaults are covered in the study paper [6]. It showcases well-known DDoS assaults, like the one carried out by Khan C. Smith in 1997, which caused a city's internet to go offline for hours, and the large attack on GitHub in 2018 that had 1.3Tbps of incoming traffic. The study focuses on the part that botnets—networks of compromised devices under an attacker's control—play in carrying out denial-of-service assaults. Various factors, such as ideological disagreements, corporate rivalry, boredom, extortion, and cyberwarfare, are behind these attacks. Volume is the primary factor used to categorize DDoS attacks, with volume-based attacks attempting to overload the bandwidth of a target server. A typical volumetric assault is the UDP flood attack, in which the attacker uses the victim's IP address as the source of fictitious UDP packets, forcing the target server to reply to these fictitious addresses.

The research paper titled "Green Cloudlet Network: A Distributed Green Mobile Cloud Network" [5] introduces a new architectural framework called Green Cloudlet Network (GCN) in the context of mobile cloud computing. This framework addresses the latency challenges of mobile cloud applications by deploying cloudlets (trusted, resource-rich computers) close to mobile devices, enabling seamless offloading of compute-intensive tasks. The concept of "avatars" is introduced. This is a software clone of your mobile device hosted on a cloudlet server. Avatars allow applications to be offloaded and run within cloudlets, reducing end-to-end latency. GCN architecture integrates green energy sources such as solar energy to minimize operational costs and reduce the carbon footprint of distributed cloudlets. To address the increasing traffic load of these distributed cloudlets, this paper proposes an SDN-based cellular core network that separates the control plane and data plane. This SDN-based approach provides efficient and flexible routing paths between endpoints, improving network performance and scalability. The paper also highlights the importance of a robust file system called Cloudlet Network File System (CNFS) to ensure low latency and data reliability for avatars.

The research paper entitled “Challenges and Research Advances in 5G Wireless Backhaul Networks” [8] addresses the complexities and advances in 5G wireless backhaul networks. With wireless communication traffic expected to increase by 2020 compared to 2010, the need for next generation 5G networks is clear. These networks are expected to increase the amount of wireless traffic by a factor of a thousand, and various transmission technologies such as Massive MIMO and mmWave communications are being explored to improve spectral efficiency and bandwidth. A key challenge addressed in this paper is the emergence of small-scale cellular networks in 5G architectures. Unlike a simple upgrade to an existing network, 5G infrastructure

requires a fundamental rethink from the system and architectural level down to the physical level. The paper emphasizes the importance of delivering hundreds of gigabits of backhaul traffic in ultra-dense cell networks while ensuring quality of service and energy efficiency. To meet these challenges, the paper discusses two primary network architectures: the central solution and the distribution solution. The central solution involves a macrocell base station collecting backhaul traffic from small cells, while the distribution solution relies on cooperative small cells forwarding traffic to a specified small cell. The energy efficiency of these solutions is thoroughly analyzed, considering both operating energy and embodied energy, offering valuable guidelines for designing energy-efficient 5G wireless backhaul networks.

The article, "SDNhome: A methodology for controlling future wireless home networks," [9] describes the challenges of managing a wireless home network with different segments controlled by different technologies. The authors propose a Software-Defined Networking (SDN) approach called SDNhome to address these challenges. They claim that SDNhome increases network flexibility and interoperability, making it easier to support a variety of home applications. The authors explore the evolution of home networking applications, from simple Internet access to more complex tasks such as multimedia streaming and home automation. These highlight the fragmentation and complexity of managing different network segments, each using different technologies, which can lead to potential conflicts and coexistence issues. To address these challenges, the paper introduces the concept of SDNhome, where a centralized control plane, managed by a network administrator, is used to program and manage various wireless devices within a home network. This approach enables flexible and dynamic programming of devices, separating control and data planes to improve network management and performance. SDNhome is presented as a way to empower the home gateway (HGW) to act as an SDN controller, unifying control under a common protocol, enabling the installation of radio programs, and dynamically configuring devices based on application scenarios and network conditions. This programmable approach aims to optimize home network performance and simplify the addition of new services.

The article describes the application of Software Defined Networking (SDN) in optical networks [4], recognizing the complexity of modern optical networks and the need for flexible control and management solutions. SDN separates the control plane from the data plane, which provides benefits for controlling, operating, and managing large networks. It's flexible, agile, and cost-effective, allowing network administrators to quickly respond to changing business needs. Modern optical networks are vast and handle large amounts of data, creating control and management challenges for carriers and providers. SDN was introduced as a framework to address these challenges. Separates control, data, and management planes to facilitate dynamic programmability and efficient network management. The article focuses on the development of SDN for optical networks, building on research dating back to around 2010. Applications of SDN in optical networks include global optical network resource optimization, cloud integration with 5G networks, data center network design, and transport network control plane frameworks. SDN is offered as a solution to simplify network control and management in optical networks. Separates data and control levels, ensuring centralized management and increasing flexibility. Standardization and interfaces like OpenFlow play a key role in enabling interoperability between network components from different vendors.

The paper describes the concept of Blockchain as a Service (BaaS) as an important development in blockchain technology. [10] This highlights the decentralization, persistence, anonymity, and auditability features of blockchain, which have led to its widespread adoption in various sectors. However, it also recognize the complexities of developing blockchain-based applications, such as the need for different agencies within the government to launch different projects. BaaS is presented as a solution to address this complexity by providing a cloud-based service that allows developers to focus on business logic without managing the underlying blockchain platform. This paper focuses on the role of large technology companies in providing BaaS, which has accelerated the adoption of blockchain technology since 2017. BaaS is described as the integration of cloud computing, Internet of Things (IoT), and edge computing, providing features such as consensus management, forking, node validity, goods exchange, and resource management. It is positioned as a way to outsource technical complexity to service providers and improve productivity in blockchain application development. This paper points out that while there is sufficient research on blockchain, research

on BaaS is limited. To fill this gap, the authors conducted a survey of over 30 of BaaS-related publications. The main contributions of this paper are presented, including a comprehensive review of various aspects of BaaS, such as architecture, service technology, and applications. The paper also discusses future challenges and research trends in the BaaS field. The architectures of both commercial BaaS systems and new academic BaaS systems are investigated. The architectures of major commercial systems such as Alibaba, IBM, Microsoft, Oracle, and Amazon are detailed, and their unique features are highlighted. Academic systems such as Novel BaaS (NBAaS), Unified BaaS (uBaaS), Functional BaaS (FBaaS), and NutBaaS have also been investigated, each offering a different approach to BaaS implementation.

The article describes the challenges faced by mobile carriers due to increased mobile Internet traffic, increased capital expenditures (CAPEX) and operating expenses (OPEX) and slowing average revenue per user (ARPU) growth [2]. This highlights the need for innovative solutions to maintain profitability and improve services. To efficiently deal with the increase in traffic, the article considers the three alternatives: increasing spectral efficiency, dynamic spectrum access, and introducing more cells with smaller size. However, it also recognize that these approaches have limitations. The article highlights the importance of energy efficiency in reducing operating costs and carbon emissions. The inefficiency of base station (BS) power consumption and the challenges arising from the increasing number of cell sites are receiving increasing attention. It introduces the concept of Cloud Radio Access Network (C-RAN) as a new architecture that leverages cloud computing and shared processing to aggregate OS computing resources into a central pool. C-RAN is presented as a solution to reduce capital and operational costs while providing better service. The proposed C-RAN logical structure includes a physical layer, a control layer, and a service layer. The focus is on service cloud, service-oriented resource planning and management concepts aimed at improving network performance for both terminals and operators.

The article titled-"D2D Communication in the Internet of Things: Traditional Communication Protocols, Challenges, and Unresolved Issues discusses the importance of device-to-device (D2D) communication as a key feature of the Internet of Things (IoT) [1]. It highlights the importance of D2D communication in improving overall throughput, spectral efficiency, and resource utilization in IoT. The introduction defines IoT as a network of intelligent devices that can communicate data over the Internet without requiring human-to-human or human-to-computer interaction. This article traces the history of D2D communications, from its introduction into wired networks to its relevance to next-generation cellular networks. This paper classifies D2D communication networks into two main structures: standalone D2D communication and network supported D2D communication. It highlights the growing need for D2D communication to ensure IoT success and indicates a growing trend in D2D communication. The main objective of study is to investigate current communication technologies and their applicability to IoT. Provides insight into various traditional communication protocols including Bluetooth, WiFi, Zigbee, NFC, Cellular, LoRaWAN, RFID, Z-Wave, Sigfox, and more. Each protocol is evaluated based on network topology, network speed, communication range, and application area.

The article describes the application of Software-Defined Networking (SDN) to Traffic Engineering (TE) in the context of modern network architectures [7]. SDN separates the control and transport layers of a network, offering benefits such as centralized control, programmability, and open interfaces. The paper provides an overview of the framework for TE in SDN, focusing on traffic measurement and traffic management. Learn about the challenges and technologies associated with network measurement, traffic analysis, and prediction in SDN. The framework aims to monitor and analyze network traffic to optimize traffic management and improve resource utilization and quality of service (QoS). Describes traditional IP-based TE and Multiprotocol Label Switching (MPLS)-based TE, along with their benefits and limitations. SDN's core control and programmability capabilities make it a promising platform for TE, providing solutions to problems such as traffic measurement and planning. However, challenges remain, such as the coexistence of SDN and traditional IP networks and the need to develop TE solutions for hybrid networks. The paper concludes that TE technology in SDN is essential for the advancement of his SDN applications in various fields.

T. Pereira, L. Barreto, and A. Amaral's paper discusses the difficulties in network and information security in the context of Industry [20]. The integration of cyber-physical systems that characterizes Industry 4.0 presents particular security challenges. The writers examine these issues and stress the necessity of strong security protocols to safeguard private data and guarantee the dependable operation of networked systems. It is probable that the paper explores particular threats like data breaches, illegal access, and possible weaknesses in the network infrastructure. In order to successfully implement and maintain Industry 4.0 technologies and contribute to a safer and more resilient industrial landscape, it is imperative that these challenges are understood and addressed.

The research paper titled "Wireless Body Sensor for Wearable Health Monitoring" [3], Remote Body Range Sensor Systems (WBASNs) empower ceaseless checking of crucial signs like ECG, EEG, EMG, and EOG. This revolutionizes healthcare. These sensors assemble data and send it to a clinical server for examination utilizing advanced mimicked insights methods. Divergent to routine, stumbling systems, WBASNs offer flexibility and long pull ease of utilize without compromising sign quality. Utilizing correspondence progressions like Bluetooth Moo Vitality (BLE), ZigBee, and Super Wide Band (UWB), WBASNs ensure moo control utilization, reliable data transmission, and similitude. They optimize vitality utilize, control temperature, and ensure QoS by utilizing an assortment of steering conventions. Key challenges consolidate channel conveyance, security, RF prosperity, normalization, and vitality capability. Tending to these will move forward WBASNs' blend with emerging 5G organizations and IoT applications, basic for moving quiet thought and prosperity checking advancement.

IV. CONCLUSION

In conclusion, the collection of research papers covers a wide range of topics in the areas of cloud computing, Internet of Things (IoT), network security, artificial intelligence, and emerging technologies such as Software-Defined Networking (SDN) and Blockchain as a Service. The study highlights the critical importance of security measures in cloud environments and proposes a framework for data protection and abuse prevention. Additionally, discussions about IoT address its potential vulnerabilities and the need for secure solutions, with a particular focus on user and end-user capabilities. Exploring SDN in a variety of contexts, such as wireless home networks and optical networks, highlights the potential of SDN to address challenges in network architecture, control, and management. The integration of visible light communications and positioning into 5G Internet of Things networks reflects continued efforts to improve the reliability, data rates, and security of new technologies. Additionally, this contribution addresses the practical aspects of the trade-off between runtime security and performance in the development of SSL/TLS protocols and adaptive security techniques. Studying trends in DDoS attacks and implementing the Green Cloudlet Network framework demonstrate our continued efforts to address emerging challenges in cybersecurity and mobile cloud computing. Additionally, contributions on traffic engineering for 5G wireless backhaul networks, wireless body area sensor networks, and SDN provide valuable insights into the complexities, advances, and future directions of these fields. A review of BaaS and proposed cloud radio access network architectures presents an innovative approach to simplify blockchain development and improve the energy efficiency of cellular networks. In summary, this study contributed to the current issues, technology advances, and potential solutions, and continuous discussions and progress in the field of information and communication technology.

V. FUTURE SCOPE

Long-standing time scope of investigate within the domain of cloud computing, IoT, biometrics, SDN, arrange security, NFV, AI, cognitive computing, SSL TLS conventions , versatile security, unmistakable light communication, DDoS assaults , green cloudlet systems , 5G remote backhaul, remote body region sensor systems , SDN in domestic systems , SDN in optical systems, Blockchain as a Benefit , portable cloud computing, and D2D communication inside the following few a long time is promising and multifaceted. Researchers ought to centre on improving the security and security measures in cloud situations, creating strong arrangements for IoT vulnerabilities, and investigating progressions in SDN to address challenges in

conventional organize models. Furthermore, future work seem dig into moving forward the vitality effectiveness of cloudlet systems, optimizing 5G remote backhaul systems, and advancing the applications of blockchain innovation. Headways in AI and cognitive computing ought to point at maximizing benefits in different commerce settings. Besides, inquire about endeavors ought to proceed to improve within the zones of arrange security, NFV applications, SSL TLS conventions, and versatile security procedures. Investigating novel approaches for joining obvious light communication and situating in 5G systems and tending to challenge in remote body range sensor systems for wearable wellbeing checking offer energizing openings. Future inquiries about ought to too center on refining SDN methodologies for controlling remote domestic systems and optical systems, as well as investigating the potential of Blockchain as a Service. In outline, end of the inquire about scene ought to prioritize security, proficiency, and imaginative applications over different spaces, guaranteeing that developing advances contribute to a more associated, secure, and productive computerized future

VI. REFERENCES

[1]. Yashoda, M., & Shivashetty, V. D2D Communication in Internet of Things: Conventional Communication Protocols, Challenges and Open Issues.

[2]. Wu, J., Zhang, Z., Hong, Y., & Wen, Y. (2015). Cloud radio access network (C-RAN): a primer. IEEE network, 29(1), 35-41.

[3]. Alrashidi, M., & Nasri, N. (2021). Wireless body area sensor networks for wearable health monitoring: technology trends and future research opportunities. International journal of advanced computer science and applications, 12(4).

[4]. Routray, S. K., Jha, M. K., Javali, A., Sharma, L., Sarkar, S., & Ninikrishna, T. (2016, August). Software defined networking for optical networks. In 2016 IEEE Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER) (pp. 133-137). IEEE.

[5]. Sun, X., & Ansari, N. (2017). Green cloudlet network: A distributed green mobile cloud network. IEEE network, 31(1), 64-70.

[6]. Rahamathullah, U., & Karthikeyan, E. (2021, May). Distributed denial of service attacks prevention, detection and mitigation–A review. In Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021) (p. 16).

[7]. Shu, Z., Wan, J., Lin, J., Wang, S., Li, D., Rho, S., & Yang, C. (2016). Traffic engineering in software-defined networking: Measurement and management. IEEE access, 4, 3246-3256.

[8]. Ge, X., Cheng, H., Guizani, M., & Han, T. (2014). 5G wireless backhaul networks: challenges and research advances. IEEE network, 28(6), 6-11.

[9]. Gallo, P., Kosek-Szott, K., Szott, S., & Tinnirello, I. (2016). SDN@ home: A method for controlling future wireless home networks. IEEE Communications Magazine, 54(5), 123-131.

[10]. Song, J., Zhang, P., Alkubati, M., Bao, Y., & Yu, G. (2022). Research advances on blockchain-as-a-service: Architectures, applications, and challenges. Digital Communications and Networks, 8(4), 466-475.

[11]. Kim, J., Manaligod, H. J. T., Lee, J., & Jo, S. (2019). Cloud Networking Computing. Wireless Personal Communications, 105, 399-404.

[12]. Yang, H., Zhong, W. D., Chen, C., & Alphones, A. (2020). Integration of visible light communication and positioning within 5G networks for internet of things. IEEE Network, 34(5), 134-140.

[13]. UM, U. I. Analysis of key research challenges for adaptive security.

[14]. da Costa, R. L., Gupta V., Gonçalves, R., Dias, Á., Pereira, L., & Gupta, C. (2022). Artificial Intelligence and Cognitive Computing in Companies in Portugal: An Outcome of Partial Least Squares—Structural Equations Modeling. Mathematics, 10(22), 4358.

[15]. Han, B., Gopalakrishnan, V., Ji, L., & Lee, S. (2015). Network function virtualization: Challenges and opportunities for innovations. IEEE communications magazine, 53(2), 90-97.

[16]. Dewangan, P. (2020). A review paper on network security and cryptography. International Journal of Science and Research (IJSR), 9(1).

[17]. Kaliyamurthy, N. M., Taterh, S., Shanmugasundaram, S., Saxena, A., Cheikhrouhou, O., & Ben Elhadj, H. (2021). Software-defined networking: An evolving network architecture—programmability and security perspective. Security and Communication Networks, 2021, 1-7.

[18]. Rode, K. N., Chiparge, A. A., Khot, S. J., & Patil, S. A. The Future of IoT and Biometrics. International Journal of Research Publication and Reviews

[19] Lamprecht, C. J. (2012). *Adaptive security* (Doctoral dissertation, Newcastle University).

[20]. Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. Procedia manufacturing, 13, 1253-1260.