A Comprehensive Review of the OSI Reference Model: From Fundamentals to Recent Advancements

Mr. Abhishek MS[1], Ms. Akanksha KJ[2], Ms. Priyanksha Das[3]
[1,2]*Student, Department of Forensic Science, School of Sciences, JAIN (Deemed-to-be University)*
[3]*Assistant Professor, Department of Forensic Science,*
School of Sciences, JAIN (Deemed-to-be University)
doi.org/10.64643/IJIRTV12I8-191809-459

***Abstract*—The OSI (Open Systems Interconnection) Reference Model by the International Organization for Standardization (ISO) in the late 1970s has been the most significant contributor to network communication protocol standardization and interoperability of various systems. The review paper outlines the OSI model's formal, seven-layered architecture, which encapsulates the data transmission complexities from the physical layer that deals with raw bits to the application layer that specifies user services. It explains the model's encapsulation and de-encapsulation processes towards data integrity and security, its role in network security with encryption, and its flexibility to accommodate new technologies. It reviews the OSI standardization challenges, compares it to practices such as TCP/IP, explores its conformity with new technologies such as wireless sensor networks and cloud computing, and its continued use in computer networking today, making it a useful reference document for researchers, practitioners, and students.**

I. INTRODUCTION

International Organization for Standardization (ISO) has developed a historic model known as the Open Systems Interconnection (OSI) reference model, making computer network understanding and designing simple (Fraihat, 2021). It was developed in the late 1970s and has a theoretical model describing a formal method of network communication and dividing it into seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application (Patil et al., 2017). The OSI model has played a crucial role in network protocol standardization, interoperation, and simple development of networking technology (Singh & Thoke, 2020). By imposing layered architecture, it simplifies the modular design complexity, where each layer is designed to perform predefined functions and communicates with neighboring layers directly using well-defined interfaces (Mahmoud & Yuan, 2011). This modularity simplicity in design simplifies network communication complexity so protocols can be designed and implemented separately for each layer (Kaur & Singh, 2012). The Physical layer manages raw data transport over physical media, while the Data Link layer offers real data transport between directly connected devices (Mekuria & Belay, 2022). The Session layer manages logical addressing, routing, and forward data delivery in a network formed by several networks (Mwafugha et al., 2014). The Transport layer comprises end-to-end communications services including segmentation, flow control, and error recovery (Alotaibi, 2021). The Session layer manages, maintains, and synchronizes communication sessions between programs (Dlodlo & Mvelase, 2013). The Presentation layer offers data representation compatibility, i.e., encoding, encryption, and compression (Gibson, 2011). Finally, the Application layer offers services and interfaces for user applications to utilize network services (Fouda et al., 2011). Since its inception, the OSI model has been a working background in computer networking research and study, serving as a tool for common communication to facilitate interoperability and network architecture or protocol communication (Sharma & Bedi, 2017). Its effects extend beyond the world of IT, as it has been used in other sectors like government and educational institutions across the globe (Kumar et al., 2014).

II. OVERVIEW OF THE OSI MODEL

The OSI (Open Systems Interconnection) model is a theoretical framework for describing and standardizing the aspects of a telecommunications or computing system. The OSI model identifies seven layers, each of which has its own purpose (Zimmermann, 1980).

- Physical Layer: The physical layer is the portion of the connection that relates to the direct connection between the devices and should also, when talking about it in terms of a connection, encompass the electrical, mechanical and procedural attributes. This also includes any connectors that can potentially be used. These, as examples would include, though their nomenclature relates to being physical, are Ethernet Cable, Fibre Optics, Wireless signals (Forouzan, 2006).

- Data Link Layer: The data link layer is, as its description reflects, is used to transfer (medium) data between two adjacent nodes on the physical layer and be able to do it in a reliable way. The data link is responsible for error detection and error recovery, flow control, framing. For elaborating we can give Ethernet and Wi-Fi as an example of protocols that operate in this layer (Tanenbaum & Wetherall, 2011).

- Network Layer: The network layer determines how packets are routed over multiple networks to get to their final destination. This layer determines the best path a packet must take to reach its destination, is responsible for logical addressing, and congestion control. The Internet Protocol (IP) operates at the network layer. (Comer, 2000)

- Transport Layer: The transport layer provides end-to-end communication between two devices. This layer provides reliable transport, in-sequence delivery, flow control, and error checking. The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) operate at the transport layer. (Kurose & Ross, 2017)

- Session Layer: The session layer is responsible for opening and closing connections between two applications. The session layer is responsible for session synchronization, checkpointing, and recovery. Examples of this layer include NetBIOS and PPTP (Point-to-Point Tunneling Protocol). (Stallings, 2007)

- Presentation Layer: This layer refers to data transformation and encryption of messages to enable reliable translation of information from one system to another. The presentation layer guarantees that formatted data can be read correctly by the receiving application layer and it also assists with encryption and compression. The presentation layer includes the encoding formats JPEG, MPEG and SSL (Ramezani & Hussain, 2010).

- Application Layer: The application layer refers to the layer that is used by end-users through applications or network services. Application protocols have a large number of functions and are composed of recommendations for email (SMTP), file transfer (FTP), and web browsing (HTTP) (Stolz, 2009).

Significance of Layered Architecture:

- Independent Protocol Evolution and Modular Design: OSI layer model offers modular protocol design. Each layer can be independently designed and extended, hence allowing new protocols and technologies to be integrated with minimal effect on the surrounding layers (Day & Zimmermann, 1983).

- Division of Responsibilities and Abstractions: The system divides the complex process of networking into individual layers, which are assigned specific functions. The division of responsibilities makes it possible for the network designers to correct one problem in the system at a time, which leads to an easier-to-understand design and makes debugging easier (Zhang, 2010).

- Standardization and Interoperability: OSI allows hardware and software interoperability among different vendors through the creation of standard interfaces among the layers. The standardization allows devices from different manufacturers to communicate properly, fostering a competitive market and innovation (ITU-T, 1994).

III. APPLICATION AND IMPLEMENTATIONS

a. Network Protocol Design and Standardization:

- TCP/IP is the primary protocol suite used by computer networks and the Internet. TCP/IP has four levels, which are the application layer, transport layer, internet layer, link layer. TCP is connection-oriented and guarantees data transfer, while IP is responsible for routing packets and addressing. Other protocols in the suite are HTTP, FTP, and SMTP (Cerf & Kahn, 1974).
- Wireless Network Protocols: Wireless networks use multiple protocols, including Wi-Fi (IEEE 802.11) for local area networking, Bluetooth to link devices over a short range, and cellular protocols, such as 4G LTE and 5G, for the wireless transmission of mobile data (Goldsmith, 2005).
- Internet of Things (IoT) Communication Protocols. IoT devices support various protocols based on their requirements, including MQTT (Message Queuing Telemetry Transport) for messaging that has a low message size, CoAP (Constrained Application Protocol) for low-resource devices, and Zigbee for low-power and low-data-rate wireless networks (Al-Fuqaha et al., 2015).

b. Network Management and Security:

- OSI Network Management Model: The OSI network management model identified five areas of function: fault management, configuration management, accounting management, performance management, and security management. These functional areas utilize the efficacy and capabilities of a network in monitoring, configuring, analyzing, and securing the network resources (ISO/IEC 7498-4, 1989).
- Security Features across OSI Layers: Security policies utilize security features that exist in all layers of the OSI model to counteract different vectors of threat. For example, firewall technologies and other types of intrusion detection systems (IDS) exist at the transport and network layers that monitor, block attack vectors, and encrypt traffic using protocol standards and specifications (Oppliger, 1997).
- Intrusion Detection Systems and Intrusion Prevention Systems: Intrusion Detection Systems and Intrusion Prevention Systems operates on the principle of detecting irregularities in network traffic and respond accordingly to the detected threats by notification to the appropriate network administrators or respond automatically to restrict or block the attack in progress. An intrusion detection system uses a combination of signature-based configuration of data monitoring, is usually event driven (anomaly) based on triggering threshold alerts, and heuristics (Scarfone & Mell, 2007).

c. Educational Tools and Learning Platforms:

- Simulation and Gaming Interactions: Students are provided with effective experiential learning in networking principles using interactive gaming and simulation websites. Packet Tracer and GNS3 are examples of software suites that allow students to simulate network configurations and troubleshoot issues in a virtual laboratory (Cisco Systems, 2019).
- Virtual Laboratories & Network Emulators: Virtual labs and network emulators can allow students (theoretically) to take risk-less approaches to testing their various network configurations and implementations without neglecting physical platforms. Using software such as VMware Workstation and VirtualBox students can use the virtualization platforms to run multiple virtual machines together (Kaur & Singh, 2014).
- Online Tutorials & Courses: There are many online tutorials, courses, and workshops available on various networking topics, some basic and some advanced protocols and technologies. Several learning platforms, including: Coursera and Udemy, offer online self-study courses, video lectures and interactive quizzes, introducing networking concepts and making learning accessible at any level (Anderson, 2020).

IV. COMPARISON WITH OTHER NETWORK MODEL

a. TCP/IP or DoD Model:

The TCP/IP or Department of Defense (DoD) model is often recognized by the unqualified name "Internet

model". It was developed prior to OSI and had a profound impact on the development of OSI. (Comer, 2000; Tanenbaum & Wetherall, 2011).

Similarities and Differences with OSI Model:

- The DOD model and the OSI model have some things in common. Both DOD and OSI provide a model for networking communication (Forouzan, 2007). However, these models are similar in one way or another as their number of layers are not only different, but the job of each layer is different, too. In the OSI model there are seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application layers. Whereas the DOD model has four layers: Application, Transport, Internet, and Link layers (Kurose & Ross, 2017; Olifer & Olifer, 2006).
- The OSI model identifies a specific function for layers, and data is sequentially carried across the layers until it reaches its destination. Whereas, the DOD model is simplified and has some of the OSI model's functions in different layers and combined (Peterson & Davie, 2011). For instance, the Application layer in the DOD model is the combination of the Application, Presentation, and Session layers found in the OSI model.
- Within the DoD model there are four layers: Application, Transport, Internet, and Network Access. In a similar fashion to OSI, it provides a framework for understanding networks and how communication over networks works, although the organization and number of layers differ from OSI (Comer, 2000). For example, the two OSI layers (Data Link and Physical) are combined in the DoD model into the Network Access layer (Peterson & Davie, 2011).
- Even though there are distinctions between the two models, both have a number of similar constructs, including ensuring the segregation of concerns and encapsulating the data as it is moved through layers (Forouzan, 2007). Both of the models facilitate interoperability by having a known interface between layers (Stallings, 2007).

Advantages and Disadvantages of Each Model:

- The OSI model is beneficial because it takes a comprehensive view of networking by promoting layered networking abstractions, separating concerns, and supporting interoperability (Stallings, 2007). However, as a complete reference model with many layers of abstraction, the implementation of OSI can be difficult to put into practice. It can also be difficult to manage the inter-layer interactions since the implementation of each layer may differ by implementation (Tanenbaum & Wetherall, 2011).
- The DOD model is advantageous because it is easier to implement and troubleshoot, and it is widely adopted (Comer, 2000). The streamlined design of DOD models aligns closely with the actual protocols in the Internet, attracting widespread adoption which increases the overall compatibility of implementations. DOD model may not be applicable in scenarios where a deeper understanding of broad networking concepts is necessary due to its lack of abstraction (Kurose & Ross, 2017).

Influence on the Development of the OSI Model:

- The DoD model was influential to the creation of the OSI model and influenced the structure of the Internet (Zimmermann, 1980). Although the OSI model was an independent invention, it was, to some degree, influenced by the DoD model and some of its ideas/constructs became the principles used to develop the OSI model. As the DoD clearly described a simple model for communication capabilities and the ability to implement procedures, and because the OSI model included and expanded upon those ideas, the DoD model influenced the OSI layer architecture with a less is more approach while allowing standardization across network communications (Olifer & Olifer, 2006).

V. ADVANTAGES AND LIMITATIONS OF THE OSI MODEL

The OSI model offers several advantages, but it also has some limitations that need to be considered they are as follows,

Flexibility and Adaptability:

- The flexibility and freedom of the OSI model, is one of the best features of it. The layering structure of the OSI model allows the new technology and protocols to be integrated without

disturbing the existing technologies (Forouzan, 2007). Each layer can be independently developed and updated (Kurose & Ross, 2017). This way new technologies and protocols can be integrated easier and without impacting the other layers. This makes it easier for equipment with includes new Layer 2 protocols, to use the same equipment as older Layer 2 devices in case of inter-operation (Peterson and Davie 2011).

Complexity and Overhead:

- Although the holistic view implemented in the OSI model may have limitations, the multi-layered design has the potential to create complexity and overhead when implemented or managed in certain situations (Stallings, 2007). The complexities arising from coordinating operations and interactions among the layers, as well as the disparate implementations from multiple vendors make implementation difficult with resource usage overhead ("Running Out of Time," 2010). The focus that the OSI model places on standardization and abstraction means that it could diverge from what is appropriate in a true opportunity situation prompting additional overhead usage (Comer, 2000).

VI. CHALLENGES AND SECURITY CONSIDERATIONS:

a. Denial of Service and Distributed Denial of Service Attacks:

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks pose significant challenges to network security, targeting various layers of the OSI model.

Types of DoS/DDoS Attacks at Different Layers:

- DoS and DDoS attacks can affect various OSI layers and utilize weaknesses in network structure and protocols. An example of this is a Flood at the network layer such as ICMP Floods and SYN Floods that create an enormous amount of data that will overwhelm the network resources and use the victim's equipment (Mirkovic & Reiher, 2004). An example of attacks at the Transport layer are TCP and UDP Floods; these attacks are intended to utilize the vulnerabilities in the implementation of protocols to use up the system resources to affect communication. At the Application layer, DoS and DDoS attacks specifically characterize attacks on services or applications, such as HTTP Floods and DNS amplification attacks, which target services to flood them with excessive requests to intentionally deny service (Douligeris & Mitrokotsa, 2004).

Mitigation Techniques and Countermeasures:

- A multi-faceted approach must be taken in order to mitigate DoS and DDoS attacks, combining both network-level solutions and application-layer protections. At the network level, techniques available include traffic filtering, traffic-rate limiting, and traffic analysis - all of which can identify malicious traffic and block it prior to reaching its intended target (Zargar et al., 2013). Network appliances can be implemented such as firewalls, routers, and intrusion detection/prevention systems (IDS/IPS) to understand traffic and mitigate DoS/DDoS attacks in real time. At the application layer, other solutions include load balancing, content distribution networks (CDNs), and application layer firewalls - all of which can help distribute incoming traffic and filter out attackers and reduce the detrimental effects of DoS/DDoS attacks on important applications/services (Kalkan et al., 2017).

b. Layer-Specific Vulnerabilities and Countermeasures:

Different layers of the OSI model are susceptible to various vulnerabilities, requiring layer-specific countermeasures to address them effectively.

Physical Layer Security:

- Because the physical layer can be devastated by physical attacks including wiretapping, eavesdropping, and electromagnetic interference, physical security measures such as cable shielding, tamper evident seals, and secure buildings can provide some level of little protection from physical attacks to the physical layer by securing physical access to network infrastructure and by preventing unauthorized physical tampering or interception of data (Stallings, 2013).

Data Link Layer Vulnerabilities and Solutions:

- The attacks on the data link layer include MAC address spoofing, ARP spoofing, and VLAN hopping. You can mitigate against these attacks using port security, MAC address filtering, dynamic ARP inspection (DAI), and VLAN access control lists (VACLs) that can be used to prevent unauthorized access and provide network segmentation as well as isolation (Zhou & Haas, 1999).

Network Layer Attacks and Defenses:

- The Service Later (Layer 3) is open to attacks like IP spoofing, routing attacks, and fragmentation attacks. These attacks could potentially be prevented and/or detected with the presence of ingress and egress filtering, anti-spoofing mechanisms, and cryptographic mechanisms such as IPsec to verify authorization, authenticity, and integrity of the contents of the network traffic and provide a secure form of communication (Kent & Atkinson, 1998; Patel et al., 2011).

c. Security Enhancement and Extension to the OSI Model:

Enhancing the OSI model with additional security mechanisms and extensions can help address emerging threats and improve the overall security posture of networked systems.

Incorporating Security Mechanisms at Each Layer:

- One way to increase the security of the OSI model is to integrate security mechanisms into each layer of the protocol stack. For example, implementing encryption and authentication protocols at the presentation layer, to secure the integrity and confidentiality of data, and using access control mechanisms at the network layer to limit access to network services based on the user and their identity and access permissions. Organizations can establish discrete features of security at the layers of each protocol and establish organizational wide security controls throughout the network layers to mitigate potential attacks that focus on particular vulnerabilities (Peterson & Davie, 2007).

Human Factors Extension for Enhanced Security:

- An additional area of consideration for improving OSI model security is human factor considerations such as user behaviors and security awareness. Human error and negligence comprised much of the root cause of security breaches, and organizations are required to devote resources towards user awareness training and programs for educating end-users on security best practices such as passwords management, phishing awareness, and social engineering. An organizational culture of security awareness and accountability can assist in fostering users to have an active role in participation of defence of cyber threats thereby reducing the chances of successful attacks (Hadlington, 2017).

Proposed 8th Layer for Tactical Wireless Networks:

- Researchers and practitioners have proposed new layers onto the OSI model in some contexts in addition to layering security functions in each layer of the OSI model. Some examples of this can be found in tactical wireless networks utilized in military and emergency services that create their own rules outside of the OSI model. Traditional OSI layers and processes cannot address the unique obstacles presented in tactical wireless such as the effects of mobility, interoperability, and resilience to interference and jamming. As a possible solution, researchers have recommended including an eighth layer specifically for tactical wireless networks (Wang et al., 2014). The proposed eighth layer would create means and protocols for managing network topology, turf management, and allocation and optimization of resources in a changing environment. In this sense, if the OSI model allows for the inclusion and clearly demonstrates the operations in tactical wireless networks, specific organizations could better ensure the reliable and secure communication needed in these conditions (Zhou & Haas, 1999).

VII. RECENT DEVELOPMENTS AND FUTURE DIRECTIONS:

a. Adaptation of the OSI model to emerging technologies:

- The OSI (Open Systems Interconnection) model, a conceptual framework for understanding and designing computer networks, has been slowly but surely adapted for emerging technologies including wireless sensor networks, software

defined networking (SDN), and cloud computing through virtualization (Tan & Liu, 2020).

Wireless Sensor Networks (WSNs):

- The traditional OSI model layers from physical to application represents a standardized methodology for communicating over a network. The WSNs are however a unique classification of network communication due to the limitations of WSNs (resource constrained device and dynamic nature of the network topology). Modifications to the OSI model, particularly in the physical and data link layers, are required for a WSN to adopt the OSI model to accommodate the WSN limitations of low-power constraints, bandwidth, and dynamic conditions of a network. Various sensors and protocols e.g., Zigbee and 6LoWPAN have been developed to assist in WSN communication by conscripting to the model data link and network layers of the OSI model with energy-efficient mechanisms i.e., sleep voltages and network re-routing as part of many WSN protocols (Al-Fuqaha et al., 2015).

Software-Defined Networking (SDN):

- SDN refers to the abstraction of the control plane (intended for data forwarding) from the management and programmability of the data forwarding plane. Centralized management and programmability can be accomplished with SDN, and although the OSI model will still be important while developing a cloud infrastructure, SDN enables an abstraction layer above the OSI model that can encompass multiple OSI layers of the model, including the data link layer (Layer 1), network layer (Layer 3), and transport layer (Layer 4). As described, the important point is that the layers should be re-examined in terms of how they should interact with each other, using the OSI model as the point of reference. For example, the SDN controller is considered the functional equivalent of the OSI network layer; an SDN controller operates at the network layer (Layer 3), while the switch (analyzers) and routers operate at the data link layer (Layer 1). An SDN controller tells the switches and routers how to set up the network path and forwarding rules. The OSI model can adapt to include SDN specific considerations employed on top of its original layers.

Cloud Computing and Virtualization:

- Cloud computing and virtualization as applied technology changes the architecture of networks by abstracting resources and allowing for flexibility to scale and grow on demand. The OSI model was designed for classic architectures and as such needs to be accounted for with cloud computing and virtualization to mitigate challenges and realize possibilities (Zhang et al., 2010).

Cloud-Based Network Architectures:

- Integrating cloud computing in the OSI model requires that we take the existing layers of the OSI and add capabilities specific to cloud services. The new application layer adds cloud services such as Software as a Service (SaaS)(Vishnu Venkatesh & Das, 2026), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS); all of which utilize virtualization technologies in a scalable adaptable manner (Zhang et al., 2010). The existing session and presentation layers of the OSI model may also include protocols and standards for secure communications and the serialization of data in a cloud computing environment (Popa et al., 2011).

Virtualization Network Function Services:

- Virtualization, by definition, is an abstraction layer that enables the separation of network functions from the physical hardware. This virtualization layer works across OSI layers enabling the deployment and management of service(s) (Han et al., 2015). Network Function Virtualization (NFV) and Virtual Network Function (VNFs)(Shukla et al., 2023), enabled by virtualization technologies enables instantiation and management of network services in dynamic way. Within the OSI model, virtualization implies redefining, and the roles of data link, application link, and transport layers to enable the construct and operation of virtualized network functions with ensuring interoperability and performance (Mijumbi et al., 2016).

b. Integration with cloud computing and virtualization:

- Integration of cloud computing and virtualization: Integration of cloud computing and virtualization and the OSI model means that the OSI model

layers will be referenced in cloud-based network architectures and virtualized network function services.(Venkatesh et al., 2023)

Cloud-Based Network Architectures:

- The layers of the OSI model, especially the application, session, and presentation layers have been extended by cloud-centric enablement's. We can also incorporate the OSI layers into the OSI model in order to describe cloud-based services such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In addition to cloud-specific functionality, the OSI model can include protocols and standards for secure communication and data serialization, in order to describe operations and services in cloud environments. We can now describe a cloud-based mechanism we can provide the applications and services we can over the OSI model with a trusted set of standards and protocols to ensure interoperability and safety.(Shenoy et al., 2025)

Virtualization Network Function Services:

- Virtualization technologies create a new layer of abstraction that spans across multiple OSI layers to enable the deployment and management of network services. When we talk about virtualization of network services in the OSI model terms we are essentially redefining the roles defined for the data link, network layer, and transport layer with an eye to the virtualization of network functions. NFV and VNFs used virtualization technologies to dynamically instantiate and manage network services with improved scalability and flexibility. By introducing virtualization to the OSI layers, it will permit network operators to better exploit usage of resources, lower operational expenses, and decrease delivery times for services (Mijumbi et al., 2016).

c. Potential improvements and modifications to the OSI model:

The OSI model continues to adapt based on new requirements and challenges and advances in the relevant technologies. Enhancements and modifications to its layers have the potential to be made.

Responding to New Requirements and Challenges:

- As network environments are becoming increasingly complex and diverse, so too will the OSI model need to change to meet new requirements and challenges. Including IoT devices, 5G networks, and edge computing in the OSI model is an example of a new challenge (Sharma et al, 2020). New protocols and standards may be created to enhance interoperability, security, and scalability at the OSI-layer application levels to support changing technology and use-cases (Liu et al, 2018).

Optimizing Performance and Efficiency:

- As the demand for ultra-high-performance networking grows, it is easy to envisage a multitude of optimizations of the OSI model to improve performance and efficiency. At each layer, protocols and algorithms can be altered or replaced as needed to achieve lower latencies, reduced overheads and optimized throughput (Kim et al, 2019). Hardware advances in hardware acceleration and network processing will add another layer of potential to uniquely address OSI-compliant systems, especially with respect to exploiting 'higher performance' via increased packet forwarding rates and effortless data transmission.

Incorporating Emerging Technologies and Trends:

- The OSI model should stay flexible to include newer technological developments and trends like: AI-enabled networking, quantum-communication, and blockchain protocols. Continuation of research and standardization as it relates specifically to incorporating new technologies into the OSI model is necessary. It may be that new layers or sublayers could create a more specialized function that would integrate within the OSI model, thus maintaining its responsibilities regarding new network paradigms.

VIII. CONCLUSION

The OSI reference model has been a fundamental component of computer networks development and standardization. The layered structure of the OSI Reference Model has been used for the design and implementation phases of many network protocols,

improved interoperability, and provided a systematic way of thinking about network communication. While there has been criticism of the model and its effect on the development of the Internet, the OSI broadens our understanding and analysis of network architectures. The OSI model has shifted as technology has advanced, both in terms of an adaptation of components and allowing for improvements over technologies that exist. Further research and development continue to evaluate how to improve the usefulness of the OSI model and address security concerns and other issues in the revolution of new types of networking and communication systems. These endeavors include adaptations of the model in the area of wireless sensor networks, software-defined networking, cloud computing, and virtualization, while managing new requirements and challenges from emerging trends. In addition, the OSI model has been instrumental to network security, with researchers suggesting security improvements and extensions to combat known vulnerabilities and attacks from the attacker's perspective at different layers. These improvements can come in the form of building security capabilities and mechanisms added at each layer, social/human considerations or adding additional layers such as in the proposed tactical wireless networks. While part of a former era, the OSI reference model framework is still foundational to computer networking education, research, and practice, and still a helpful framework to enhance an understanding of creating a more robust, secure, and interoperable network architecture. The clear, modular, and layered nature of the OSI model still holds relevancy for identifying current and possible future security vulnerabilities and exposures in an increasingly digital world.

REFERENCES

[1] Li, Y., Li, D., Cui, W., & Zhang, R. (2011). Research based on OSI model. In 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN) (pp. 554–557). Xi'an, China. doi:10.1109/ICCSN.2011.6014631

[2] Shukla, M., Srivastav, V., Khare, M. D., & Venkatesh, N. V. (2024). IoT-Driven solutions for VANET trustworthiness: Examining misconduct and position security challenges. Multidisciplinary Reviews, 6, 2023ss059.

[3] Alani, M. M. (2014). Guide to OSI and TCP/IP Models. Springer Briefs in Computer Science. doi:10.1007/978-3-319-05152-9_2

[4] Vishnu Venkatesh N., Singhal, P., Pandey, D., Sharma, M., Rautdesai, R., Khubalkar, D. N., & Gupta, A. (2023). Crime Forecasting Using Historical Crime Location Using CNN-Based Images Classification Mechanism. In B. Pandey, D. Pandey, R. Anand, D. Mane, & V. Nassa (Eds.), Handbook of Research on Thrust Technologies' Effect on Image Processing (pp. 206-221). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-6684-8618-4.ch013

[5] Mr. N VISHNU VENKATESH, Dr. Asha Rajiv, Ms. Priyanksha Das, Mr. Shreyas Warrier (2026). Vantage Point Recreation: A Novel Approach in Endpoint Security for Smart Homes. International Journal of Innovative Research in Technology (IJIRT), 12(8), 6226-6235.

[6] SUNIDHI SUDHEER SHENOY, N VISHNU VENKATESH, "A Predictive Framework for Real-Time Courtroom Assistance Using AI-Based Mock Legal Advisor", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.12, Issue 2, Page No pp.440-444, May 2025

[7] Day, J. D., & Zimmermann, H. (1983). The OSI Reference Model. Proceedings of the IEFJ2, 71(12), 8 pages. Invited Paper.

[8] Saxena, P. (2014). OSI reference model–a seven layered architecture of OSI model. International Journal of Research (IJR), 1(10), 1145-1156.

[9] Zimmermann, H. (1980). OSI reference model-the ISO model of architecture for open systems interconnection. IEEE Transactions on communications, 28(4), 425-432.

[10] Yemini, Y. (1993). The OSI network management model. IEEE Communications Magazine, 31(5), 20-29.

[11] Fraihat, A. (2021). Computer networking layers based on the OSI model. Test Eng. Manag, 83, 6485-6495.

[12] Day, J. (1995). The (un) revised OSI reference model. ACM SIGCOMM Computer Communication Review, 25(5), 39-55.

[13] Kumar, S., Dalal, S., & Dixit, V. (2014). The OSI model: Overview on the seven layers of computer networks. International Journal of Computer Science and Information Technology Research, 2(3), 461-466.

[14] Handel, T. G., & Sandford, M. T. (1996, May). Hiding data in the OSI network model. In International Workshop on Information Hiding (pp. 23-38). Berlin, Heidelberg: Springer Berlin Heidelberg.

[15] Kritzinger, P. (1986). A performance model of the OSI communication architecture. IEEE transactions on communications, 34(6), 554-563.

[16] Jasud, P. V. (2017). The OSI Model: Overview on the Seven Layers of Computer Networks. International Journal for Innovative Research in Science & Technology, 4(3), 116-124.

[17] Uiphanit, T., Bhattarakosol, P., Suanpong, K., & Iamsupasit, S. (2019). Packet warriors: An academic mobile action game for promoting OSI model concepts to learners.

[18] Raman, L. (1998). OSI systems and network management. IEEE Communications Magazine, 36(3), 46-53.

[19] Khaing, E. E. (2019). Comparison of DOD and OSI Model in the Internet Communication. International Journal of Trend in Scientific Research and Development (IJTSRD) Volume, 3, 2574-2579.

[20] Orzen, S. N. (2014, May). Interaction understanding in the OSI model functionality of networks with case studies. In 2014 IEEE 9th IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI) (pp. 327-330). IEEE.

[21] Bauer, B., & Patrick, A. S. (2004). A human factors extension to the seven-layer OSI reference model. Retrieved January, 6, 2004.

[22] Turay, B. (2019). Analysis of Seven Layered Architecture of OSI Model. Journal For Innovative Development in Pharmaceutical and Technical Science (JIDPTS), 2(12).

[23] Salvi, M. V., & Bapat, M. P. Mode of Data Flow in the OSI Model. International Journal of Innovations in Engineering Research and Technology, 2(3), 1-7.

[24] Zhao, J., Bai, J., Zhang, Q., Yang, F., Li, Z., Zhang, X., ... & Bai, R. (2018, December). The discussion about mechanism of data transmission in the OSI Model. In 2018 International Conference on Transportation & Logistics, Information & Communication, Smart City (TLICSC 2018) (pp. 1-4). Atlantis Press.

[25] Abdul, A. M., & Umar, S. (2017). Attacks of Denial of Service on networks layer of OSI model and maintaining of security. Indonesian Journal of Electrical Engineering and Computer Science, 5(1), 181-186.

[26] De Prycker, M., Peschi, R., & Van Landegem, T. (1993). B-ISDN and the OSI protocol reference model. IEEE Network, 7(2), 10-18.

[27] Suresh, P. (2016). Survey on seven layered architectures of OSI model. International Journal of research in computer applications and robotics, 4(8), 1-10.

[28] Kumar, G. (2014). Understanding denial of service (dos) attacks using osi reference model.

[29] International Journal of Education and Science Research, 1(5).

[30] Ashford, C. (1993, July). The OSI Managed-object Model. In European Conference on Object Oriented Programming (pp. 185-196). Berlin, Heidelberg: Springer Berlin Heidelberg.

[31] Nuangjamnong, C., Maj, S. P., & Veal, D. (2008, September). The osi network management model-capacity and performance management. In 2008 4th IEEE International Conference on Management of Innovation and Technology (pp. 1266-1270). IEEE.

[32] Zhou, M., Zhou, M., & Zhu, E. (2014). Information and Communication Technology for Education. WIT Press/Computational Mechanics.

[33] Kalyanasundaram, P., & Sethi, A. S. (1993). An Application Gateway Design for OSI-Internet Management. Integrated Network Management, 3(C-12), 389-400.

[34] Meyer, D., & Zobrist, G. (1990). TCP/IP versus OSI. IEEE Potentials, 9(1), 16-19.

[35] Bordetsky, A., & Hayes-Roth, R. (2007). Extending the OSI model for wireless

battlefield networks: a design approach to the 8th Layer for tactical hyper-nodes. International Journal of Mobile Network Design and Innovation, 2(2), 81-91.

[36] Gallert, G. P. (2010). Mapping network protocols to layers of the osi model. International Magazine on Advances in Computer Science and Telecommunications, 1(1), 31.

[37] Pavlou, G., McCarthy, K., Bhatti, S., & Knight, G. (1995). The OSIMIS platform: Making OSI management simple. In Integrated Network Management IV: Proceedings of the fourth international symposium on integrated network management, 1995 (pp. 480-493). Springer US.

[38] Pardue, M. D. (1987, October). Fine-tuning the osi model: Layer functions and services. In MILCOM 1987-IEEE Military Communications Conference-Crisis Communications: The Promise and Reality (Vol. 1, pp. 0199-0203). IEEE.

[39] Ceballos, S. S., & Leyva, J. A. L. (2015, October). An optimized collaborative platform for educational cloud computing in application and presentation layers of OSI model. In 2015 International Conference on Computing Systems and Telematics (ICCSAT) (pp. 1-5). IEEE. Mayukha, S., & Vadivel, R. Various Possible Attacks and Mitigations of the OSI Model Layers Through Pentesting–An Overview.

[40] McBrien, P. (1997). Design of distributed applications based on the OSI model. In Advanced Information Systems Engineering: 9th International Conference, CAiSE'97 Barcelona, Catalonia, Spain, June 16–20, 1997 Proceedings 9 (pp. 361-373).

[41] Springer Berlin Heidelberg, Bochmann, G. V. (1990). Protocol specification for OSI.

[42] Computer Networks and ISDN Systems, 18(3), 167-184.

[43] Barzola, J., & Rubini, L. (2014, November). The telegestore system evolved according OSI model and its performance compared with the new IEEE 1901.2 standard. In 2014 IEEE Central America and Panama Convention (CONCAPAN XXXIV) (pp. 1-4). IEEE.

[44] Santos, M. G. M., & Marcillo, P. A. A. (2018). Security in the data link layer of the OSI model on LANs wired Cisco. Journal of Science and Research, 3(CITT2017), 106-112.

[45] Kayri, M., & Kayri, İ. (2010). A proposed" OSI Based" network troubles identification model. arXiv preprint arXiv:1009.6045.

[46] Lewan, D., & Long, H. G. (1983). The OSI file service. Proceedings of the IEEE, 71(12), 14141419.

[47] Swetha, M. S., Thungamani, M., & Krishnan, K. (2018). A Survey on different types of MANET attacks in OSI model. Int. J. Innovative Res. Sci. Technol., 4, 18-23.

[48] Conway, A. E. (1989, June). Performance modeling of multi-layered OSI communication architectures. In IEEE International Conference on Communications, World Prosperity Through Communications, (pp. 651-657). IEEE.

[49] Obaid, H. S., & Abeed, E. H. (2020). DoS and DDoS attacks at OSI layers. International Journal of Multidisciplinary Research and Publications, 2(8), 1-9.

[50] Bolanowski, M., Paszkiewicz, A., Zapala, P., & Żak, R. (2014). Stress test of network devices with maximum traffic load for second and third layer of ISO/OSI model. Pomiary Automatyka Kontrola, 60.

[51] Martinović, M., Lovaković, D., & Ćosić, T. (2014). Network Security Issues in Regard to OSI Reference Model Layers. In Proceedings of TEAM 2014 6 th International Scientific and Expert Conference of the International TEAM Society 10–11 th November 2014, Kecskemét, Hungary (p. 105).

[52] Mughal, A. A. (2020). Cyber Attacks on OSI Layers: Understanding the Threat Landscape.

[53] Journal of Humanities and Applied Science Research, 3(1), 1-18.

[54] Razumov, P., Lyashenko, K., Cherckesova, L., Revyakina, E., Yengibaryan, I., & Revyakin, A. (2023). Development of a system for protecting against DDoS attacks at the L7 level of the OSI model-HTTP Flood. In E3S Web of Conferences (Vol. 402, p. 03008). EDP Sciences.

[55] Amin, M. S., & Rahman, S. (2023). An Introduction of Open System Interconnection (OSI) Model and its Architecture.

[56] Kaur, D., & Singh, P. (2014). Various OSI layer attacks and countermeasure to enhance the performance of WSNs during wormhole attack. International Journal on Network Security, 5(1), 62.