Smart and Secured Healthcare System

Prashant Uppar[a], Pratiksha Angadi[b], Chandni Kumari[c], Swapnil Shahapurkar[d]
and U. V. Somanatti[e]

Department of Computer Science and Engineering, KLE Tech, University's Dr. MSSCET, Belagavi, India

Keywords: Network, Security, IOT, Automation, OSPF, Routing, ASA Firewall, VPN, Remote Login.

Abstract: The growing reliance on digital infrastructure in healthcare institutions necessitates robust solutions to address data security and operational efficiency. This paper presents a smart and secure healthcare network framework that integrates advanced firewall configurations, dynamic routing protocols, and IoT enabled safety automation. The proposed system ensures data confidentiality, integrity, and availability by implementing optimized OSPF routing, multi layered traffic filtering through firewalls, and secure remote access using VPN with SSH encryption. IoT technologies enhance hospital safety by enabling automated fire detection, temperature control, and smoke detection systems. Experimental results validate the efficiency of this framework in mitigating unauthorized access, streamlining network management, and automating safety measures. This approach offers a scalable and effective solution to modern healthcare challenges, emphasizing secure communication and reliable automation.

1 INTRODUCTION

The healthcare sector is increasingly dependent on digital technologies to manage patient data, streamline hospital operations, and automate various safety measures. However, the digitization of healthcare has also led to the exponential growth of sensitive information, making these networks prime targets for cyber attacks and unauthorized access (Sendelj and Ognjanovic, 2022). These vulnerabilities not only compromise patient privacy but can also disrupt hospital operations, potentially leading to severe consequences for both patients and healthcare providers. Therefore, it is paramount to implement robust security measures that protect critical data and ensure the continuous operation of healthcare systems (Namoğlu and Ulgen, 2013). Despite the growing importance of network security, existing systems often fail to sufficiently address the complex needs of modern healthcare environments. Healthcare networks are usually large and involve various interconnected devices, systems, and departments. This complexity increases the difficulty of ensuring secure data transmission, maintaining privacy, and safeguarding against unauthorized intrusions. Moreover, many traditional security mechanisms struggle to balance cost efficiency, scalability, and flexibility, often requiring expensive infrastructure or overly simplistic solutions that fail to meet all requirements (Wazid et al., 2022).

One of the key challenges in securing healthcare networks is the diverse range of communication protocols and devices in use, coupled with misconfigurations in routing and inadequate traffic filtering. These gaps can result in data breaches, downtime, and system vulnerabilities, putting sensitive patient information at risk. Furthermore, the integration of Internet of Things (IoT) technologies into hospital operations such as smart fire detection systems, temperature regulation, and smoke detection adds another layer of complexity. While these devices can automate safety features and improve operational efficiency, they also introduce new security risks, particularly in terms of secure communication and remote access (Alsbou et al., 2022). The proposed work addresses these issues by designing a Smart and Secured Healthcare System that aims to improve both the security of hospital data and the automation of essential safety functions. The system employs several advanced techniques, including optimized dynamic routing with OSPF, advanced firewall configurations, and IoT-based automation for fire detection, tempera-

[a] https://orcid.org/0009-0004-2892-9636
[b] https://orcid.org/0009-0003-2499-1646
[c] https://orcid.org/0009-0004-0613-7574
[d] https://orcid.org/0009-0004-4044-4324
[e] https://orcid.org/0000-0002-6930-6628

Uppar, P., Angadi, P., Kumari, C., Shahapurkar, S. and Somanatti, U. V.
Smart and Secured Healthcare System.
DOI: 10.5220/0013600000004664

In *Proceedings of the 3rd International Conference on Futuristic Technology (INCOFT 2025) - Volume 2*, pages 676-684
ISBN: 978-989-758-763-4

ture control, and smoke monitoring. These features work together to provide a comprehensive solution that not only secures hospital data but also ensures operational efficiency and safety (Alsbou et al., 2022).

The key objectives of this work are, **Network Security,**To design and implement a secure network architecture for a hospital environment, using subnetting for network segmentation, static routing for initial traffic management, and dynamic OSPF routing to ensure optimized, efficient data transfer across departments. **Traffic Filtering and Intrusion Prevention,** To deploy advanced firewall mechanisms that filter traffic, monitor network activity, and prevent unauthorized access, ensuring that only authorized personnel and devices can access the hospital's internal systems. **Remote Access Security,** To ensure secure, encrypted communication for remote access to hospital systems via VPN and SSH encryption. The use of VPN provides a secure tunnel for all internet traffic, while SSH is used for secure remote command execution and system management. **IoT-Based Automation,** To integrate IoT technologies for automating safety operations within the hospital, including systems for fire detection, temperature regulation, and smoke detection. These systems will operate in real time, ensuring the safety of patients and hospital infrastructure.

The structure of the paper is organized as follows: Section 2 reviews related work, emphasizing limitations in current approaches and how the proposed work addresses these gaps. Section 3 details the methodology, including network configuration and IoT-based safety integration. Section 4 presents the results, analyzes performance and accuracy, and compares the proposed system to existing solutions. Section 5 concludes the paper with a summary of contributions, key findings, and recommendations for future research.

2 RELATED WORKS

The evolution of healthcare systems has driven extensive research in security, IoT integration, and automation. Existing studies explore various methodologies, including blockchain, firewalls, and smart IoT systems, to enhance data privacy, network security, and operational efficiency. While advancements like Healthcare 5.0 and medical IoT platforms showcase potential, gaps such as scalability, real world validation, and emerging technologies persist. This survey consolidates insights to guide future implementations addressing these challenges.

In (Priya et al., 2017) reviewed security attacks in electronic healthcare systems, discussing security requirements such as authentication, integrity, and confidentiality. They categorized attacks based on the data phases of gathering, transmission, and storage. The study offers a comprehensive categorization of security attacks, emphasizing the importance of multi layered security and theoretical insights. However, it lacks practical implementation, experimental validation, and quantitative benchmarks. The gaps identified include the absence of specific solutions, a lack of integration with emerging technologies like AI or blockchain, and limited adaptability to real time threats.

In (Jin et al., 2019) conducted a survey of secure and privacy preserving medical data sharing mechanisms, with a focus on blockchain based approaches. They categorized the mechanisms into permissionless and permissioned types and analyzed techniques such as cryptography, anonymization, and SDN. The review highlights the potential of blockchain in healthcare, especially in cryptographic solutions and SDN integration. However, it relies on off chain storage due to blockchain limitations, lacks real world implementation, and does not use a specific dataset. The study identifies challenges in ensuring fine grained access control, compatibility across domains, and the need for a unified query mechanism, as well as holistic solutions integrating blockchain with cryptography and SDN.

In (Makhdoomi et al., 2022) reviewed conventional and next generation firewalls (NGFWs), their deployment methods, and comparative features. They explored distributed firewalls and NAT/PAT firewalls, highlighting the advanced features of NGFWs such as IPS and application layer filtering. While the study provides a thorough theoretical review, it lacks practical implementation and experimental results. Gaps include insufficient research on distributed firewall policies, topologies, and effective real world implementations of access control mechanisms.

In (Sendelj and Ognjanovic, 2022) systematically analyzed cybersecurity challenges in healthcare, identifying risks, consequences of attacks, and best practice recommendations. The study offers a comprehensive overview, leveraging recent statistical data to provide actionable insights. However, it is primarily descriptive, lacks empirical testing of solutions, and does not cover all emerging technologies. The gaps identified include the need for case studies on successful implementations, exploration of emerging technologies, and research on the effectiveness of proposed frameworks.

In (Wazid et al., 2022) proposed a secure framework for Healthcare 5.0, analyzing its applications, security requirements, threat models, and existing mechanisms. The framework provides a robust approach to addressing security challenges and compares existing performance metrics. However, it remains theoretical, with no extensive empirical validation. Gaps include the need for practical case studies, exploration of emerging technologies, and further research on framework effectiveness.

In (Pandey et al., 2020) conducted a systematic literature review and scientometric analysis to assess healthcare data integrity techniques. The study offers a roadmap for future research by highlighting effective techniques like blockchain. However, it is limited by a focus on previously used methods and a lack of exploration of new approaches. The gaps include a need for comprehensive studies addressing multifaceted data integrity challenges in healthcare.

In (Namoğlu and Ulgen, 2013) conducted a case study in a 150 bed private hospital in Turkey, examining vulnerabilities in hospital information systems and proposing a secure network infrastructure. The study identifies security vulnerabilities and provides best practices based on standards like HIPAA and ISO 80001. However, the lack of extensive sample data and security concerns in revealing the hospital's identity are limitations. Gaps include insufficient compliance with healthcare standards, inadequate staff training, and a lack of privacy agreements with external users.

In (Alsbou et al., 2022) designed and simulated an IoT based smart hospital using Cisco Packet Tracer. The system integrates IoT devices like sensors and actuators for real time patient data transmission. It enhances patient care and response times, but the simulation is limited by scalability challenges, network congestion, and insufficient evaluation of data security in complex environments. Gaps include the need for real world testing, scalability assessment, and advanced security measures for IoT based systems.

In (Walia et al., 2023) developed a safe and secure smart home using IoT technology in Cisco Packet Tracer. The system includes RFID based access control, burglary detection, fire and smoke systems, and water and temperature monitoring. The study enhances security and safety but relies heavily on stable internet connections and lacks features like voice recognition or predictive analytics. Gaps include robust cybersecurity measures, scalability exploration, and advanced features for smart home ecosystems.

In (Fu et al., 2023) developed a comprehensive Medical IoT platform to unify healthcare scenarios and devices, addressing data fragmentation through technical standards. The platform supports seamless data collection, real time decision making, and health data fusion but faces challenges with interoperability and validation of data reliability. Gaps include insufficient device integration, improved data sharing standards, and comprehensive evaluations of platform effectiveness in real world settings.

In (Roy et al., 2023) implemented a smart home automation system in Cisco Packet Tracer, integrating IoT devices for fire safety and enhanced network security. While the system provides comprehensive automation, it is limited by simulation constraints and device interoperability challenges. Gaps include further research on real world applicability, advanced security measures, and diverse IoT device integration for enhanced functionality.

In (Karunamurthy et al., 2023) implemented the Routing Information Protocol (RIP) for managing IoT devices across different LANs. The study highlights enhanced IoT management and automation but focuses on simulation in controlled environments. Gaps include research on scalability and emerging technologies for better IoT management solutions.

In (Yudidharma et al., 2023) conducted a systematic literature review to analyze messaging protocols and electronic platforms for smart homes. The study identifies commonly used protocols like MQTT and CoAP and evaluates performance. However, it focuses on existing literature, leaving gaps in emerging technologies and user centric solutions.

In (Abdunabi et al., 2023) developed a secure system architecture for Body Area Networks (BAN), incorporating Spatio Temporal Attribute Based Access Control (STABAC) and blockchain for policy integrity. While the study enhances healthcare data management, it lacks performance evaluation and consideration of insider threats. Gaps include assessments of mobile user access and the proposed model's real world effectiveness.

In (Madhav et al., 2023) designed and simulated a smart hospital using IoT technologies in Cisco Packet Tracer. The system integrates automation for safety and security but lacks real world deployment, predictive analytics, and scalability for larger hospital networks. Gaps include real time patient monitoring, advanced predictive models, and integration of speech recognition and machine learning for smart hospitals.

In (Alzu'bi et al., 2024), a systematic literature review was conducted to define research questions, formulate keywords, filter articles, and classify results. This study provides a comprehensive overview of privacy and security concerns in edge computing, identifying key privacy needs and discussing potential solutions. However, the study is limited in its focus on practical implementations and does not explore other computing paradigms in detail. The research identifies a significant gap in privacy-preserving strategies and integration studies for intelligent edge systems in healthcare applications.

In (Samudrala et al., 2024), IoT devices were integrated using Cisco Packet Tracer for centralized fire detection employing a star topology. This methodology enhances fire detection through the use of smoke and motion sensors, enabling real-time alerts and monitoring. Despite its advantages, the study is simulation-based and does not fully address real-world variables. Further research is necessary to test this system in real-world scenarios and integrate it with other safety measures.

In (Salunkhe et al., 2024), the use of microservices in healthcare was analyzed, particularly for clinical applications. This approach improves scalability, maintainability, and responsiveness within healthcare systems. Nevertheless, challenges persist regarding data consistency, security compliance, and integration with legacy systems. Future studies should focus on empirical evaluations and strategies for integrating user experiences into microservice architectures.

In (Khan et al., 2024), a home server using PCIe technology for Network Attached Storage (NAS) was designed, and performance comparisons were conducted. The findings emphasize the benefits of scalability, centralized management, and data security. However, the study has limited consideration of energy efficiency and potential security vulnerabilities. Further research is recommended to develop energy-efficient solutions and conduct real-world analyses of such systems.

In (Ghasab et al., 2024), a centralized virtual network for fire stations in Iraq was proposed using Cisco Packet Tracer. This approach aims to improve emergency coordination, response times, and resource allocation. However, the study lacks a detailed analysis of server failures and the resilience of the proposed network to cyber threats. Further investigation is required to evaluate the network's impact and incorporate enhanced security measures.

In reviewing the existing literature and approaches, it is evident that current healthcare systems face significant limitations, particularly in areas such as network segmentation, security, scalability, and IoT integration. Many systems rely on flat network topologies, outdated security protocols, and manual monitoring, which can lead to performance bottlenecks, data vulnerabilities, and slower response times during emergencies. Furthermore, existing systems often lack scalability, requiring expensive overhauls to accommodate growing needs. The proposed System addresses these gaps by implementing advanced network management techniques like subnetting and dynamic routing, enhancing security with modern encryption and automated access controls, integrating IoT devices for real time monitoring and response, and ensuring scalability and cost efficiency for long term adaptability.

3 PROPOSED METHODOLOGY

Fig.1, illustrates the logical architecture of the proposed system, focusing on how different layers and components interconnect to achieve efficient healthcare network management. This design emphasizes the conceptual structure and modularity of the system, ensuring scalability, reliability, and security across all layers

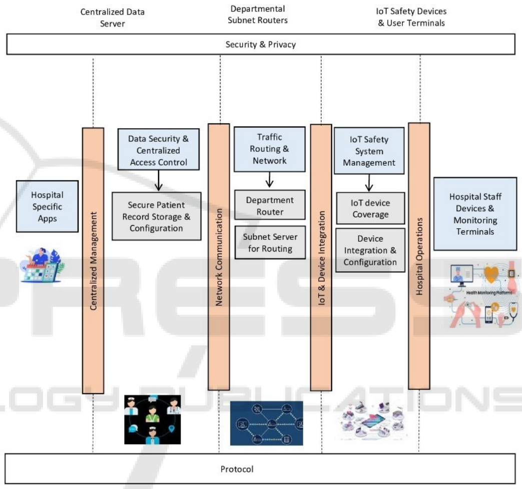

Centralized Data Server
Departmental Subnet Routers
IoT Safety Devices & User Terminals
Security & Privacy
Hospital Specific Apps
Centralized Management
Data Security & Centralized Access Control
Secure Patient Record Storage & Configuration
Network Communication
Traffic Routing & Network
Department Router
Subnet Server for Routing
IoT & Device Integration
IoT Safety System Management
IoT device Coverage
Device Integration & Configuration
Hospital Operations
Hospital Staff Devices & Monitoring Terminals
Health Monitoring Platforms
Protocol

Figure 1: Logical Architecture of the Proposed System

Centralized Management layer ensures secure storage of patient data, centralized configuration, and access control. It acts as the primary control hub for the entire system. Network Communication Comprising departmental subnet routers and traffic routing mechanisms, this layer manages data flow and network connectivity across departments. IoT and Device Integration section is dedicated to integrating IoT safety devices and ensuring seamless device configuration and coverage for real time operations. Hospital Operations is Focused on hospital staff and monitoring systems, this layer supports applications that facilitate operational workflows and device interactions. Security and Privacy ,Spanning all layers, this ensures robust encryption, firewalls, and authentication mechanisms, safeguarding the system from vulnerabilities. This logical design serves as a blueprint, providing a high level view of how the system functions conceptually.

The logical design has been seamlessly translated into a virtual implementation using Cisco Packet Tracer. This practical setup incorporates the configuration of essential networking components, including routers, switches, IoT devices, and safety systems, while closely aligning with the blueprint provided by the logical architecture. The representation of the Cisco Packet Tracer implementation is shown below in Fig 2.

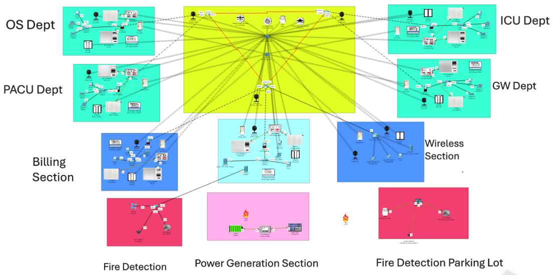


Figure 2: Cisco Network Implementation and Architecture

Centralized Core Network represents the backbone of the network, hosting the central data server and managing communication between subsystems and Configured with routing protocols (e.g., OSPF) to optimize data flow and ensure redundancy. Departmental Subnetworks are segregated based on hospital departments, each with its own routers, switches, and IoT devices. and Dynamic routing protocols and firewalls are implemented to ensure secure communication and adaptability to varying network demands. In Safety and Automation Systems, IoT enabled safety mechanisms include fire detection, temperature control, and smoke detection systems. and Devices are connected through IoT protocols and integrated with monitoring dashboards for real time alerts. In Interconnectivity, all systems are interconnected via secure VPN tunnels and encrypted communication channels to safeguard sensitive data. Load balancing ensures high availability and fault tolerance across departments. This design emphasizes modularity, scalability, and security, aligning with the logical architecture's blueprint while addressing real world constraints.

In the proposed healthcare system, OSPF (Open Shortest Path First) routing ensures dynamic and efficient communication across hospital subnetworks. It connects departmental routers to the centralized data server, enabling optimal data flow for IoT devices and monitoring systems. OSPF dynamically calculates the shortest, most reliable paths for data, adapting to changes like link failures or congestion to maintain uninterrupted healthcare operations. Its hierarchical structure segments the network into zones, reducing routing overhead while ensuring high speed communication. This protocol facilitates seamless integration of IoT sensors for fire detection, temperature control, and patient safety, ensuring robust connectivity, operational efficiency, and scalability.

VPN (Virtual Private Network) establishes a secure and encrypted connection between devices over an untrusted network, such as the internet. It ensures that data exchanged between endpoints remains confidential and protected from unauthorized access. By creating a private network tunnel, VPNs prevent potential threats like eavesdropping or data interception. VPN is utilized to safeguard communication between hospital networks and remote users. This implementation provided encrypted channels for accessing sensitive information like patient records, ensuring secure data exchange across different departments and external entities. The use of SSH (Secure Shell) encryption further enhanced the security of the VPN by adding an additional layer of protection to data transfers, ensuring only authorized users could access the network resources.

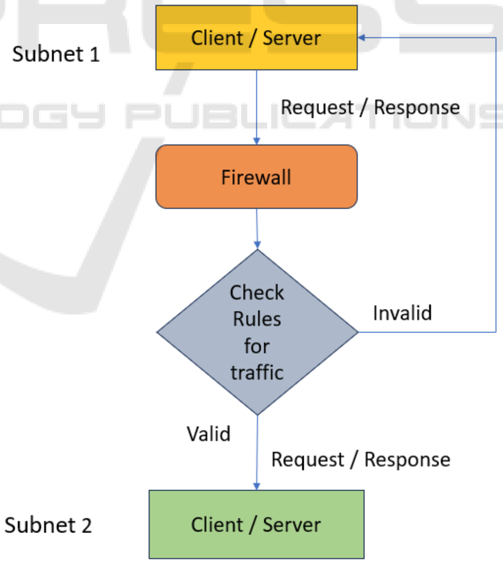


Figure 3: Firewall Traffic Filtering.

As shown in Fig. 3, the firewall acts as a security barrier between Subnet 1 and Subnet 2, monitoring and controlling data flow based on predefined rules. Requests and responses passing through the firewall are evaluated against these rules to determine their validity. Valid traffic is allowed to proceed, ensuring seamless communication between clients and servers, while invalid traffic is blocked to protect the network from unauthorized access or malicious activity. This configuration safeguards sensitive data, prevents potential breaches, and ensures compliance with security policies. Additionally, the firewall enforces traffic filtering and access control.

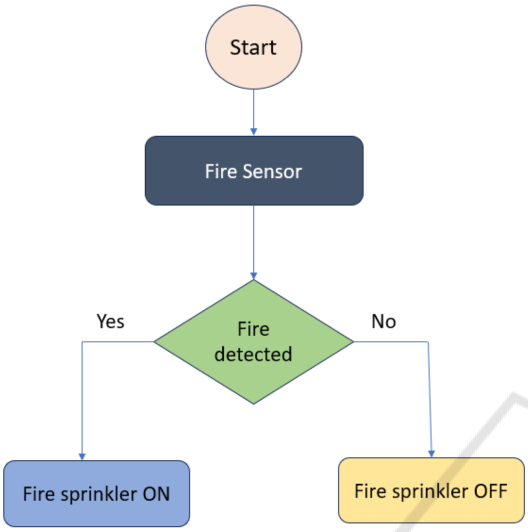


Figure 4: Fire Detection.

As shown in Fig. 4, the diagram illustrates the process of fire detection and response. The system begins with a fire sensor monitoring the environment for potential fire events. If the sensor detects a fire, it triggers the activation of the fire sprinkler system to mitigate the threat. If no fire is detected, the sprinklers remain inactive, ensuring resource efficiency. This automated system collects real time environmental data to promptly identify fire hazards. Upon detection, sprinklers are activated to minimize damage and enhance safety. The integration ensures seamless coordination and effective hazard management.

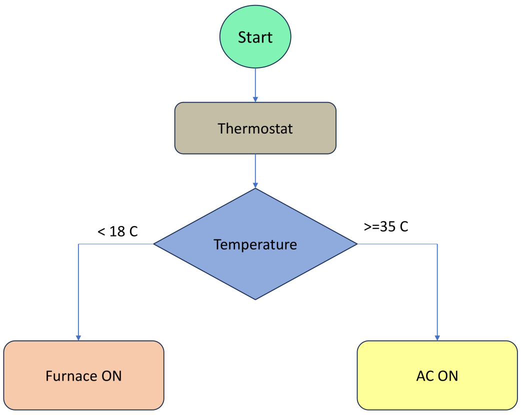


Figure 5: Temperature Control.

As shown in Fig. 5, the diagram depicts the monitoring and control of temperature through a thermostat. The system evaluates the temperature and initiates corresponding actions. If the temperature falls below 18°C, the furnace is activated to maintain warmth. Conversely, if the temperature reaches or exceeds 35°C, the air conditioning (AC) is turned on to cool the environment. This setup automates temperature-based actions to maintain optimal environmental conditions. By dynamically controlling the heating and cooling systems, it ensures effective resource utilization while addressing extreme temperature scenarios efficiently.

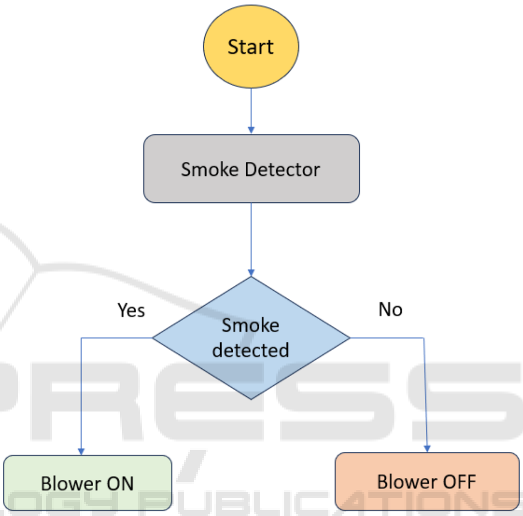


Figure 6: Smoke Detection.

As shown in Fig. 6, the diagram illustrates a smoke detection system. The process begins with a smoke detector monitoring the environment. If smoke is detected, the system activates a blower to mitigate the smoke and improve air quality. If no smoke is detected, the blower remains off to conserve energy and resources. This configuration ensures timely detection and response to smoke, preventing potential hazards while maintaining efficient operation in normal conditions. The automated control enhances environmental safety by addressing smoke related risks effectively.

4 RESULTS AND DISCUSSION

As shown in Fig. 7, The graph illustrates the accuracy and efficiency of OSPF routing over a 24 hour period, with packets sent, delivered, and overall efficiency analyzed. High alignment between pack-

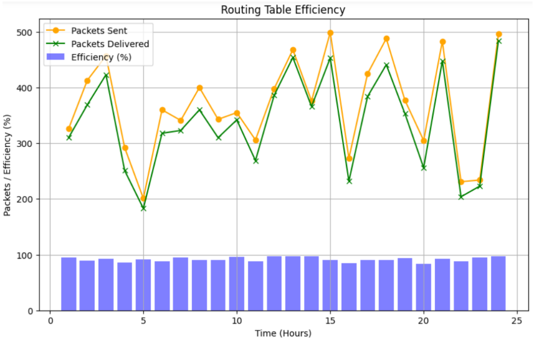


Figure 7: OSPF Routing Accuracy Analysis

ets sent and delivered demonstrates OSPF's ability to adapt to dynamic network conditions by maintaining updated routing tables. Efficiency remains consistent at most intervals, reflecting stable network performance, while occasional drops, such as at hours 5 and 20, suggest transient issues like increased network traffic or link updates. These variations highlight the protocol's robustness in maintaining data flow despite disruptions. The consistent performance underscores the reliability of OSPF in ensuring accurate packet delivery and optimal resource utilization across diverse conditions.

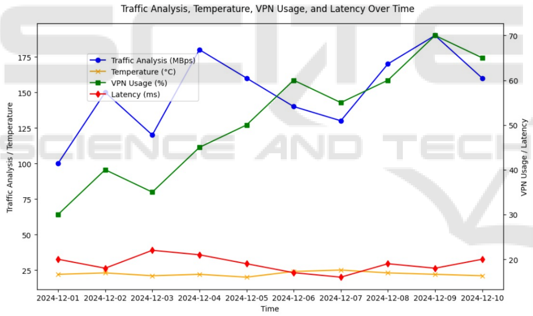


Figure 8: Temperature, VPN Success, Network Traffic and Latency Analysis Over Time

As shown in Fig. 8, The graph showcases the interplay between traffic analysis (in Mbps), temperature (°C), VPN usage (%), and latency (ms) within the configured smart healthcare system. An upward trend in traffic analysis and VPN usage is observed, indicating increased network activity and secure communication demands during peak operational periods. Despite the rise in traffic, latency remains consistently low (around 20–25 ms), signifying efficient traffic management and robust VPN implementation. Temperature, a critical IoT metric, remains relatively stable, reflecting the efficacy of temperature control systems. The synchronization between high VPN usage and minimal latency highlights the VPN's effectiveness in securely transmitting data without significant delays. These results validate the system's capability to handle dynamic workloads while ensuring data security and system performance.

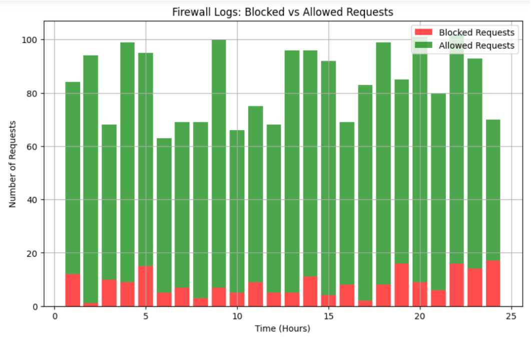
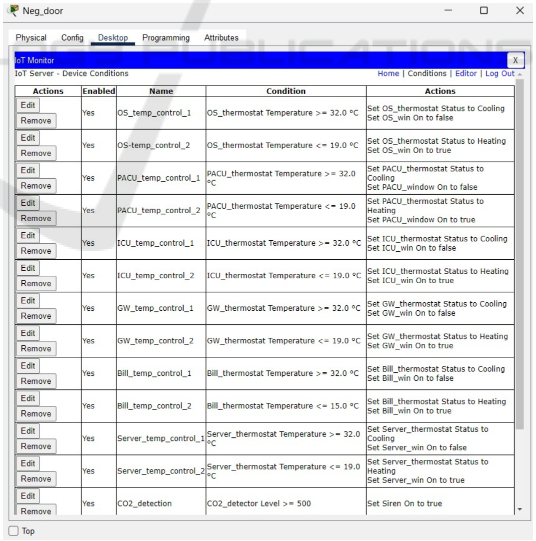


Figure 9: Firewall Traffic Filtering Analysis

As shown in Fig. 9, graph represents firewall activity within the Smart and Secured Healthcare System over a 24 hour period, highlighting the number of blocked and allowed requests. Red bars correspond to blocked requests, representing unauthorized access attempts or malicious traffic, while green bars depict legitimate requests from authorized users and devices. The consistent blocking pattern, with occasional peaks, underscores the firewall's role in safeguarding network traffic and maintaining the healthcare system's secure operation.



IoT Server - Device Conditions

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	OS_temp_control_1	OS_thermostat Temperature >= 32.0 °C	Set OS_thermostat Status to Cooling Set OS_win On to false
Edit Remove	Yes	OS-temp_control_2	OS_thermostat Temperature <= 19.0 °C	Set OS_thermostat Status to Heating Set OS_win On to true
Edit Remove	Yes	PACU_temp_control_1	PACU_thermostat Temperature >= 32.0 °C	Set PACU_thermostat Status to Cooling Set PACU_window On to false
Edit Remove	Yes	PACU_temp_control_2	PACU_thermostat Temperature <= 19.0 °C	Set PACU_thermostat Status to Heating Set PACU_window On to true
Edit Remove	Yes	ICU_temp_control_1	ICU_thermostat Temperature >= 32.0 °C	Set ICU_thermostat Status to Cooling Set ICU_win On to false
Edit Remove	Yes	ICU_temp_control_2	ICU_thermostat Temperature <= 19.0 °C	Set ICU_thermostat Status to Heating Set ICU_win On to true
Edit Remove	Yes	GW_temp_control_1	GW_thermostat Temperature >= 32.0 °C	Set GW_thermostat Status to Cooling Set GW_win On to false
Edit Remove	Yes	GW_temp_control_2	GW_thermostat Temperature <= 19.0 °C	Set GW_thermostat Status to Heating Set GW_win On to true
Edit Remove	Yes	Bill_temp_control_1	Bill_thermostat Temperature >= 32.0 °C	Set Bill_thermostat Status to Cooling Set Bill_win On to false
Edit Remove	Yes	Bill_temp_control_2	Bill_thermostat Temperature <= 15.0 °C	Set Bill_thermostat Status to Heating Set Bill_win On to true
Edit Remove	Yes	Server_temp_control_1	Server_thermostat Temperature >= 32.0 °C	Set Server_thermostat Status to Cooling Set Server_win On to false
Edit Remove	Yes	Server_temp_control_2	Server_thermostat Temperature <= 19.0 °C	Set Server_thermostat Status to Heating Set Server_win On to true
Edit Remove	Yes	CO2_detection	CO2_detector Level >= 500	Set Siren On to true

Figure 10: Temperature Control and Smoke Detection Rules

As shown in Fig. 10, IoT configuration in Cisco Packet Tracer automates temperature control and smoke detection across different areas in a smart and secure healthcare network. The system uses thermostats and windows to regulate temperature within specified ranges for critical zones such as operating rooms (OS), ICUs, PACUs, and general wards (GW). For instance, when the temperature exceeds 32°C, cooling is activated, and windows close; when it drops below 19°C, heating is enabled, and windows open. Additionally, a CO2 detector monitors air quality, triggering an alarm if levels exceed 500 ppm, ensuring prompt action for safety. This setup enhances environmental control and safety in healthcare facilities.

The comparison of the proposed System to existing healthcare solutions , Network Configuration and Routing in the proposed system utilizes subnetting and OSPF for efficient data flow and reduced congestion. In contrast, existing systems often use flat topologies, leading to bottlenecks and poor scalability due to lack of dynamic routing. Security and Traffic Management are strengthened in the proposed system through VPN with SSH encryption and a robust firewall. Existing systems typically rely on basic security protocols and lack modern encryption, making them more vulnerable to breaches. Integration of IoT and Smart Features enhances safety in the proposed system with automated IoT devices like fire detection and temperature control. Many existing systems still use manual monitoring methods, which are prone to delays and human error. Scalability and Adaptability are built into the proposed system, allowing easy expansion with new devices and protocols as the hospital grows. Existing systems often struggle to scale, requiring costly upgrades due to rigid architectures. Cost Efficiency of the proposed system leverages existing infrastructure and optimizes resources, reducing both upfront and long term costs. Existing systems tend to have high initial costs and ongoing maintenance expenses, with limited scalability.

5 CONCLUSION

In conclusion, this paper presented the design and implementation of a Smart and Secured Healthcare System, integrating advanced networking technologies such as OSPF routing, VPN with SSH encryption, and IoT based safety features. The system demonstrated efficient routing, secure data transmission, and reliable environmental monitoring, as evidenced by the performance analysis of network traffic, latency, and IoT metrics. Key findings include the robustness of OSPF routing in dynamic environments, the effectiveness of VPN in ensuring data confidentiality, and the stability of IoT driven temperature and smoke control systems. Future research could explore the implementation of the system with upcoming protocols to enhance scalability and adaptability further.

REFERENCES

Abdunabi, R., Basnet, R., and Amin, M. A. (2023). Secure access control for healthcare information systems: A body area network perspective. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 1036–1045.

Alsbou, N., Price, D., and Ali, I. (2022). Iot-based smart hospital using cisco packet tracer analysis. In *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, pages 1–6.

Alzu'bi, A., Alomar, A., Alkhaza'leh, S., Abuarqoub, A., and Hammoudeh, M. (2024). A review of privacy and security of edge computing in smart healthcare systems: Issues, challenges, and research directions. *Tsinghua Science and Technology*, 29(4):1152–1180.

Fu, L., Lin, Q., Li, C., Liu, A., Liu, X., Yang, H., and Li, H. (2023). Medical iot platform with its applications in total course of disease and health management. In *2023 8th International Conference on Communication, Image and Signal Processing (CCISP)*, pages 41–47.

Ghasab, W. H., Hadi, A. A., Alshami, A. G., Radhi, A. D., Al-Amri, R. M., and Mousa, A. H. (2024). Construction a virtual central network for all iraq's fire station. *Babylonian Journal of Internet of Things*, 2024:151–160.

Jin, H., Luo, Y., Li, P., and Mathew, J. (2019). A review of secure and privacy-preserving medical data sharing. *IEEE Access*, 7:61656–61669.

Karunamurthy, A., Victoire, T. A., Vasuki, M., and Britto, V. L. (2023). Managing iot devices with routing information protocol. *A Journal for New Zealand Herpetology*, 12(02):2643–2651.

Khan, M. F., Hazela, B., Pandey, D., Singh, K. K., and Singh, S. (2024). Design of a home server employing pcie. *International Journal of Telecommunications & Emerging Technologies*, 10(1):1–12p.

Madhav, G. S., Kommana, C., Chandana, B. S., and Khanna, M. (2023). Design and simulation of a healthcare unit. In *2023 IEEE 3rd International Conference on Technology, Engineering, Management for Societal impact using Marketing, Entrepreneurship and Talent (TEMSMET)*, pages 1–6.

Makhdoomi, A., Jan, N., Handa, P., and Goel, N. (2022). Conventional and next generation firewalls in network security and its applications. pages 964–969.

Namoğlu, N. and Ulgen, Y. (2013). Network security vulnerabilities and personal privacy issues in healthcare information systems: A case study in a private hospital in turkey. *Studies in health technology and informatics*, 190:126–128.

Pandey, A., Khan, A., Abushark, Y., Alam, M. M., Agrawal, A., Kumar, R., and Khan, P. R. (2020). Key issues in healthcare data integrity: Analysis and recommendations. *IEEE Access*, 8:40612–40628.

Priya, R., Sivasankaran, S., Ravisasthiri, P., and Sivachandiran, S. (2017). A survey on security attacks in electronic healthcare systems. In *2017 International Conference on Communication and Signal Processing (ICCSP)*, pages 0691–0694.

Roy, B., Nivethika, S. D., Manju, G., and Pandian, M. S. (2023). Comprehensive smart home automation: Network setup, fire prevention, and network security using cisco packet tracer. In *2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS)*, pages 1–4.

Salunkhe, V., Daram, S., Mehra, A., Jain, S., and Agarwal, R. (2024). Leveraging microservices architecture in healthcare: Enhancing agility and performance in clinical applications. *Available at SSRN 4985002*.

Samudrala, S. S. H., Thambi, J., Vadluri, S. R., Rajagopal, S. M., and Bhaskaran, S. (2024). Iot-based fire alarm system and motion detector: A comprehensive protocol analysis for enhanced performance. In *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, pages 1–6.

Sendelj, R. and Ognjanovic, I. (2022). *Cybersecurity Challenges in Healthcare*, volume 300.

Walia, S., Iyer, T., Tripathi, S., and Vanaparthy, A. (2023). Safe and secure smart home using cisco packet tracer. *arXiv preprint arXiv:2304.11827*.

Wazid, M., Das, A. K., Mohd, N., and Park, Y. (2022). Healthcare 5.0 security framework: Applications, issues and future research directions. *IEEE Access*, 10:129429–129442.

Yudidharma, A., Nathaniel, N., Gimli, T. N., Achmad, S., and Kurniawan, A. (2023). A systematic literature review: Messaging protocols and electronic platforms used in the internet of things for the purpose of building smart homes. *Procedia Computer Science*, 216(1):194–203.