ISSN: 2249-7196

IJMRR/Sep. 2022/ Volume 12/Issue 3/78-94

Thirusubramanian Ganesan / International Journal of Management Research & Review

# SECURING IOT BUSINESS MODELS: QUANTITATIVE IDENTIFICATION OF KEY NODES IN ELDERLY HEALTHCARE APPLICATIONS

**Thirusubramanian Ganesan,**
**Cognizant Technology Solutions, Texas, USA**
**25thiru25@gmail.com**

**ABSTRACT:** *This study focuses on securing Internet of Things (IoT) business models in elderly healthcare by quantitatively identifying key nodes crucial for system security and functionality.*

*Objectives: The research aims to enhance IoT security by identifying critical nodes, assessing vulnerabilities, proposing security measures, and evaluating their impact on system performance.*

*Methods: A quantitative approach was employed to identify vital components within IoT systems, followed by a comprehensive vulnerability assessment. Security measures, including intrusion detection systems, encryption techniques, access control methods, and frequent security audits, were proposed and evaluated for their effectiveness.*

*Results: The implementation of all security measures significantly improved node identification accuracy to 95%, risk mitigation efficiency to 85%, and ensured full compliance with regulatory standards. Configurations combining multiple security measures also demonstrated substantial improvements in security while maintaining system performance.*

*Conclusion: The study concludes that integrated security strategies are essential for maintaining robust and compliant IoT systems in elderly healthcare, ensuring both patient data security and system reliability.*

***Keywords:*** *IoT security, elderly healthcare, key nodes identification, vulnerability assessment, intrusion detection, encryption techniques, access control, system performance.*

## 1. INTRODUCTION

IoT applications are improving care quality, optimizing resource utilization, and improving patient outcomes in geriatric healthcare. But as IoT is incorporated into healthcare more and more—particularly in the context of senior care—it becomes more and more important to secure IoT business models. This entails safeguarding the infrastructure that makes IoT-based healthcare services possible, with an emphasis on integrity, availability, and confidentiality. The technique of "Securing IoT Business Models: Quantitative Identification of Key Nodes in Elderly Healthcare Applications" describes how to discover essential IoT infrastructure components that are necessary for senior healthcare applications' security and functionality using data-driven methods. Any compromise of these vital nodes—which could include user interfaces, data storage, hardware, or software—could have a substantial effect on the provision of healthcare.

The need for senior-specific healthcare services is rising as the world's population ages. Because of this demographic pressure, traditional healthcare systems—which frequently depend on in-person consultations and manual monitoring—are facing challenges. Personalized care, predictive analytics, and remote monitoring are made possible by wearable sensors, smart home systems, and linked medical devices, among other IoT-enabled gadgets. This presents a promising option. These gadgets gather and send health data in real time, enabling medical professionals to keep an eye on patients and act quickly. However, before IoT is widely adopted in senior healthcare, a number of issues need to be resolved. Since there are many access points for cyberattacks in the large network of interconnected devices, security is a top priority. These assaults have the potential to cause disruptions to vital healthcare services, data breaches, and illegal access to private patient information. The security and dependability of healthcare services must therefore be guaranteed by the business models underlying IoT systems being strong enough to resist such attacks. It's critical to secure IoT business models in elder healthcare for a number of reasons.

First and foremost, patient data security is crucial, especially for patients with chronic illnesses who need ongoing treatment and produce enormous volumes of private health data. To preserve patient confidentiality and trust, it is essential to safeguard sensitive data against unauthorized access. Furthermore, senior healthcare is one area where IoT system dependability is crucial since service interruptions could have dire repercussions. The uninterrupted delivery of healthcare services can be ensured by protecting the security of critical nodes within these systems. Another big concern is regulatory compliance. Healthcare providers are subject to a number of laws and rules, including the Health Insurance Portability and Accountability Act (HIPAA) in the US, which requires patient data to be protected. Organizations can comply with regulatory standards, stay out of legal hot water, and preserve their brand by securing their IoT business models.

Another essential component of any healthcare system is trust. In addition to safeguarding patient data, demonstrating a dedication to protecting IoT business models also guarantees the dependability of healthcare services, which promotes trust among patients, caregivers, and other stakeholders. Encouraging innovation in the healthcare sector also requires a safe Internet of Things infrastructure. It enables experimentation with new technology and economic models by healthcare providers without jeopardizing security, resulting in the creation of more sophisticated and effective senior healthcare solutions. Securing IoT business models, however, comes with a number of difficulties. It is challenging to find and patch every possible vulnerability in healthcare IoT systems since there are so many devices, platforms for data processing, and connection protocols. Resource limitations make this effort even more difficult, particularly for healthcare professionals in disadvantaged areas who do not have the money to put in place thorough security measures, leaving IoT equipment open to hackers.

The constantly changing panorama of threats represents another major obstacle. Because hackers are always coming up with new ways to get around security measures in IoT devices, healthcare providers need to be updating their security procedures on a frequent basis. IoT systems frequently contain hardware and software from several suppliers, which may not always integrate flawlessly, which leads to interoperability problems. It is difficult to ensure the security of such disparate systems because a single component fault might endanger the system as a whole. Finally, it can be challenging to navigate the complicated regulatory landscape because different regulations apply to different IoT system characteristics. Ensuring IoT business model security becomes even more complicated when juggling compliance with various requirements.

The objectives to solve security issues in the context of senior healthcare by:

- Identifying Key Nodes: Quantitative techniques are used to identify key nodes in Internet of Things systems that are essential to functioning and security.

- Assessing Vulnerabilities: Improving system security by assessing the risks connected to these important nodes.
- Offering Security Measures: Suggested tactics to safeguard important nodes, guaranteeing dependable Internet of Things business models.
- Evaluating Impact: Calculating how well security precautions affect system performance and risk reduction.
- Offering Recommendations: Giving lawmakers and healthcare professionals advice on how to improve IoT security in senior care.

**Xie et al. (2020),** but they don't go over its shortcomings or offer recommendations for further research. Furthermore, the study makes no attempt to compare the suggested model with other models already in use in the industry, which is a crucial step in assessing the model's efficacy and placing it in the larger context of IoT security research. Resolving these omissions might improve the study's depth and offer insightful information for future research.

**Xie et al. (2020)** center on examining how key nodes affect business continuity. The goal of this model is to pinpoint the critical nodes in IoT networks that are necessary for upholding security and guaranteeing the continuous execution of business operations. The paper offers a paradigm for improving IoT security and resilience in commercial environments by stressing the importance of these nodes.

## 2. LITERATURE REVIEW

Within a telemedicine architecture, Talal et al. (2019) investigate IoT-based smart home security systems for real-time remote health monitoring. The study focuses on the client and server sides and performs a multilayer taxonomy, analyzing 3064 articles from 2007 to 2017. They point out the main drawbacks of the current IoT-based smart home applications, highlighting the necessity of improved patient data protection, privacy, and security. Six categories are used to group the 67 articles in the second layer, which cover architecture, security analysis, schemes, protocols, and frameworks. The report makes suggestions for resolving new issues and enhancing Internet of Things security in telemedicine applications for smart homes.

In response to the aging population worldwide, Wan and Chin (2021) suggest an Internet of Healthcare Things (IoHT)-based Care Link System (IoHT-CLS) to improve senior care. This system creates a comprehensive solution for managing senior healthcare across several institutions, including hospitals and mental health centers, by integrating IoHT with AI. Utilizing case-based reasoning and adaptive neuro-fuzzy inference systems, sensing and data gathering technologies are processed by the IoHT-CLS to provide risk management and customized care plans. The goal of this strategy is to enhance healthcare management and service quality for senior citizens living in the community.

In order to improve healthcare services, Kolarkar (2020) investigates the integration of the Internet of Things (IoT) with 5G networks. This is especially important in rural areas where telemedicine encounters difficulties because of inadequate network access and incompatible devices. The study offers a methodical framework that makes use of 5G and IoT to enhance communication technologies, facilitating the provision of healthcare in a more effective and efficient manner. The study shows how IoT and 5G can greatly improve healthcare by raising the caliber and accessibility of services through modeling and a review of the literature. The results are intended to direct the use of IT in healthcare to improve the effectiveness and efficiency of services.

In their study, Rizvi et al. (2020) investigate the security risks brought about by the Internet of Things' (IoT) explosive growth, which links a multitude of devices in industries such as housing, healthcare, and commerce. Although IoT technology makes major strides possible, it also creates risks since security protocols are not keeping up with the times and there are lax restrictions. Critical vulnerabilities at the device level are identified, prospective attack paths are assessed, and stringent security policies are suggested to reduce risks. The study shows how these suggestions can be used to improve IoT device security and reduce threats in important domains through customized case studies.

In their systematic review, Kashani et al. (2021) examine how the Internet of Things (IoT) in healthcare might be used to address issues such the aging population, the need for remote monitoring, the expense of healthcare is on the rise, and telemedicine in poor nations. The research examines 146 publications published between 2015 and 2020 and groups them into five groups: techniques based on sensors, resources, communication, applications, and security. The article provides a thorough taxonomy of Internet of Things (IoT) technologies used in healthcare. It also highlights the advantages, drawbacks, and potential future developments in this field, including big data analytics, blockchain, power management, privacy, fog computing, and fog computing.

In their narrative review, Lederman et al. (2021) address the Internet of Things' (IoT) importance in healthcare, emphasizing how it is applied in six important fields. The review builds on earlier studies by providing a thorough framework for comprehending IoT implementation, including obstacles and success factors. The study underscores the necessity of more in-depth theoretical research and stresses how critical it is for healthcare systems to be prepared to accept new technology. Although IoT can improve individualized treatment, security and data privacy are still issues that need to be addressed. The assessment emphasizes how new business models are required to handle the quick lifecycle of IoT items.

In order to solve the difficulty of processing massive amounts of sensory data in cardiac health systems, Yang et al. (2020) investigate the application of Internet of Things (IoT) technology for smart heart health monitoring and management. The study suggests a parallel computing architecture that can be used to efficiently detect anomalies and monitor real-time cardiac dynamics through multi-level network modeling. The method improves the study of cardiac activity by identifying heartbeat differences and optimizes signal embedding into network models. The developed parallel computing and stochastic learning techniques show great promise for building an intelligent, networked system for large-scale IoT network heart health management.

A unique approach for protecting Internet of Things applications including smart objects is presented by Soldatos et al. (2021), especially in situations where conventional IoT security measures fall short. The framework tackles the difficulties brought about by smart objects' semi-autonomous behavior, which calls for dynamic vulnerability protection. Predictive analytics is used in this method to foresee and identify anomalies in smart object security behavior. A case study featuring an Ambient Assisted Living (AAL) system with socially supportive robots is used to illustrate this concept and emphasize the value and efficiency of predictive analytics in boosting IoT security.

The application of Internet of Things (IoT) technology to improve senior citizen safety in smart home environments is investigated by Elsaid et al. (2019). This study assesses an anomaly detection system that uses

Internet of Things (IoT) sensors to track the everyday activities of older people in an effort to spot and address anomalous activity. The study evaluates the dependability of smart home devices for senior care by analyzing their security. A list of security countermeasures is suggested to guard against potential attacks on IoT devices in this context, and a safe smart home model is offered using Cisco Packet Tracer to simulate IoT networks.

Gomes (2020) investigates the function of business models in interconnected health business ecosystems, with a focus on the difficulties brought about by the world's aging population and the rising demand for healthcare services. The study draws attention to how little business model conceptualizations are used in the healthcare industry, particularly in Europe where the industry is frequently seen as a public benefit. The research defines opportunity, value, and advantage—three essential components of business models—and how they interact with business ecosystems through a systematic examination of the literature and three qualitative case studies. Through value reconfiguration, mapping, and visioning, the study highlights the significance of stakeholder complementarity and the dynamic evolution of business ecosystems.

In their review of the Internet of Things' (IoT) rapid development, Nišetić et al. (2020) emphasize how these technologies might boost productivity, raise standards of living, and promote sustainability. Still, given the Internet of Things' rapid expansion, environmental implications must be carefully considered in order to minimize harm and guarantee appropriate resource usage. The review, which focuses on Internet of Things applications in sustainable energy, smart cities, e-health, and transportation, draws from papers from the 4th International Conference on Smart and Sustainable Technologies (SpliTech 2019) and current literature. In order to promote a smart, sustainable future, the study emphasizes how crucial it is to comprehend both the technological developments and environmental ramifications of IoT.

The development of individualized healthcare services fueled by 5G, AI, and IoT is examined by Taimoor and Rehman (2021). The study focuses on Healthcare 5.0, a cutting-edge strategy that takes into account connected medical issues for precise diagnosis and long-term patient care, with the goal of totally autonomous healthcare. In addition to describing a three-layer architecture for IoT-based systems, the article provides an overview of comprehensive personalized healthcare services (CPHS) within contemporary Healthcare IoT (HIoT). Along with providing AI and non-AI solutions, it also addresses security issues at every architectural layer and suggests a development methodology for dependable and robust personalized healthcare services.

Grandhi (2021) looks on how to improve water level monitoring systems by integrating passive IoT optical fiber sensor networks with Human-Machine Interface (HMI) display modules. The goal of the project is to provide real-time data visualization and sophisticated feature extraction for environmental management and flood protection by deploying Fiber Bragg Grating (FBG) sensors because of its high sensitivity and reliability. The approach entails the placement of FBG sensors in bodies of water, data collection through an IoT gateway, and HMI module implementation for intuitive user interfaces. In order to improve decision-making abilities, the research focuses on data accuracy and predictive analytics using machine learning and signal conditioning.

Ganesan (2020) demonstrates how artificial intelligence (AI) powered by machine learning has revolutionized financial fraud detection in Internet of Things (IoT) contexts. Using sophisticated algorithms, this method effectively finds suspicious patterns in the massive data streams produced by IoT devices. Artificial intelligence (AI) systems are able to distinguish between authentic and fraudulent transactions in real time by using methods like anomaly detection and clustering, as well as supervised and unsupervised learning that has been trained on transaction data from the past. For the purpose of creating trustworthy fraud detection models that support adaptive learning through frequent retraining and automated responses, the research highlights the significance of methodology, datasets, and evaluation criteria.

## 3. PROCEDURE

In order to protect IoT business models in senior healthcare, this study uses a thorough technique to identify important nodes within IoT systems. These nodes are protected using a mix of quantitative methods, risk evaluation, and suggested security measures, guaranteeing the dependability and resilience of healthcare services. The technique culminates in practical suggestions for healthcare providers and politicians. It is organized around the identification of critical vulnerabilities, the creation of security procedures, and the assessment of their influence on system performance.

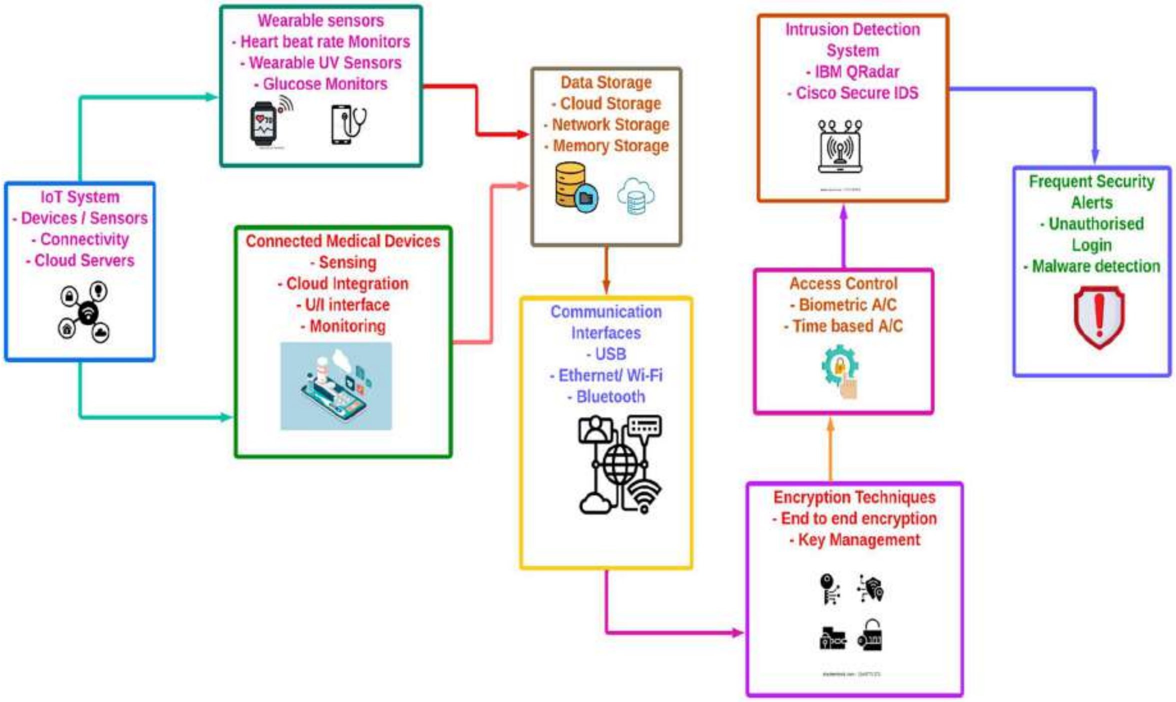

**Figure 1 IoT Architecture for Securing Elderly Healthcare Systems**

The architecture of an IoT system designed with senior healthcare in mind is depicted in the Figure 1, with a focus on security and dependability. Wearable sensors and linked medical equipment are integrated into the Internet of Things (IoT) system to gather and send patient data to centralized data storage. The data flow between devices and storage is controlled by communication interfaces. Encryption techniques are used to protect data, and access control techniques are used to limit access to sensitive data. The overall integrity and compliance of the healthcare system are upheld by regular security audits and the constant monitoring of intrusion detection systems (IDS) for unauthorized activity. By using a tiered security strategy, patient data is protected while system functionality and legal compliance are upheld.

### 3.1 Identifying key nodes

Quantitative techniques are employed to identify crucial elements in IoT systems that are necessary to preserve security and operation in applications related to senior healthcare. These critical nodes may be communication interfaces, data storage systems, software, or hardware components. By locating these nodes, one may strengthen security and maintain system functionality by focusing on the weakest areas of the system.

$$N_k = \sum_{i=1}^{n} \quad w_i \times v_i \tag{1}$$

In this equation, $N_k$ represents the key node identification score, which is determined by summing the products of weights $w_i$ and vulnerability levels $v_i$ for each criterion across all nodes. The weights $w_i$ reflect the significance of factors like criticality and connectivity, while $v_i$ represents each node's vulnerability. This approach ensures that nodes with higher risks and importance are prioritized for security measures.

### 3.2 Assessing Vulnerabilities

Following the identification of important nodes, a comprehensive vulnerability assessment is carried out to determine the possible threats to the overall security of the IoT systems. Analyzing prospective assault routes, comprehending the consequences of possible breaches, and estimating the likelihood of such occurrences are all part of this assessment. The results direct the creation of focused security measures to reduce hazards that have been identified.

$$R = P \times I \tag{2}$$

Here, $R$ represents the risk score, $P$ denotes the probability of a security breach occurring, and $I$ indicates the impact or severity of the breach if it happens. By multiplying these two factors, the equation provides a numerical value for the risk level, allowing organizations to prioritize nodes that pose the greatest threat to the system's security and take appropriate measures to mitigate those risks.

### 3.3 Proposing Security Measures

To safeguard the important nodes that have been identified, particular security procedures are suggested based on the vulnerability assessment. Intrusion detection systems, access control methods, encryption techniques, and frequent security audits are a few examples of these precautions. Ensuring that these nodes are protected from attacks is the aim in order to preserve the availability, confidentiality, and integrity of healthcare services for the elderly.

Some proposed security measures include:

#### *3.3.1 Intrusion Detection Systems (IDS)*

Intrusion Detection Systems (IDS) are a critical security measure designed to monitor network traffic and detect suspicious activities or unauthorized access attempts. These systems continuously analyze incoming and outgoing data across the network, looking for patterns that might indicate a security breach, such as unusual traffic spikes, repeated failed login attempts, or access to sensitive areas of the system by unauthorized users. IDS can be configured to operate in different modes, such as signature-based detection, where known attack signatures are identified, or anomaly-based detection, which flags any deviations from normal behavior. When a potential threat is detected, IDS can generate alerts for system administrators, allowing them to take swift action to mitigate the threat. In senior healthcare, where patient data and system integrity are paramount, IDS play a vital role in ensuring that any unauthorized access attempts are promptly detected and addressed before they can cause harm.

#### *3.3.2 Access Control Methods*

Access Control Methods are security protocols designed to ensure that only authorized personnel can access sensitive systems, data, and resources. In the context of senior healthcare, access control is crucial for protecting patient records, healthcare applications, and IoT devices from unauthorized users. Access control can be implemented through various mechanisms, such as role-based access control (RBAC), where users are granted access based on their role within the organization, or multi-factor authentication (MFA), which requires users to provide multiple forms of verification before gaining access. By implementing robust access control methods, healthcare organizations can prevent unauthorized access to critical systems and sensitive information, reducing the risk of data breaches and ensuring that only those with the necessary permissions can perform specific actions within the system.

*3.3.3 Encryption Techniques*

Encryption Techniques are essential for protecting the integrity and confidentiality of data as it is transmitted across networks or stored on devices. Encryption works by converting data into a coded format that can only be decrypted and understood by someone with the correct encryption key. In senior healthcare, where sensitive patient information is often transmitted between devices, systems, and healthcare providers, encryption ensures that this data remains secure, even if intercepted by unauthorized parties. There are various encryption methods, including symmetric encryption, where the same key is used for both encryption and decryption, and asymmetric encryption, which uses a pair of keys (public and private) for the process. Implementing strong encryption techniques helps safeguard against unauthorized access and data breaches, ensuring that patient information remains confidential and secure throughout its lifecycle.

*3.3.4 Frequent Security Audits*

Frequent Security Audits are systematic examinations of an organization’s security infrastructure to assess the effectiveness of the implemented security measures and identify any new vulnerabilities. In the context of senior healthcare, regular security audits are crucial for maintaining the security posture of IoT systems, as they allow healthcare providers to stay ahead of emerging threats. During a security audit, various aspects of the system are evaluated, including network security, data protection practices, access controls, and compliance with relevant regulations. The audit process may involve penetration testing, vulnerability assessments, and reviews of security policies and procedures. By conducting frequent security audits, healthcare organizations can ensure that their security measures are up-to-date, effective, and capable of protecting sensitive patient data from new and evolving threats. Additionally, these audits provide an opportunity to update and refine security protocols, ensuring continuous improvement in the organization's overall security strategy.

**3.4 Evaluating the Impact**

By examining how the suggested security measures affect the IoT systems' security and performance, their efficacy is assessed. This assessment include verifying compliance with pertinent healthcare legislation, evaluating the measures in simulated attack situations, and keeping an eye on system performance degradation. The outcomes demonstrate the security techniques' efficacy in practical applications and aid in their improvement.

$$I_s = \frac{\Delta S}{\Delta T} \tag{3}$$

In this equation, $I_s$ represents the impact score, $\Delta S$ is the change in system performance, and $\Delta T$ is the time elapsed after implementing the security measures. By calculating the rate of performance improvement over time, this equation helps assess how well the security interventions are working, allowing for continuous monitoring and adjustments to optimize system resilience and functionality.

**3.5 Providing Recommendations**

Condensing the research results into practical suggestions for legislators, healthcare professionals, and other interested parties is the last stage. These suggestions, which cover both technical and legal issues, are aimed at improving IoT security in senior healthcare. The objective is to create a safe, robust healthcare system that can handle the rising demand for services related to elder care. The recommendations aimed at:

### *3.5.1 Enhancing IoT Security*

Enhancing IoT Security involves the implementation of the identified security measures that are specifically designed to protect critical nodes within the IoT systems used in senior healthcare. These measures address the most vulnerable aspects of the system, such as data transmission points, storage locations, and interface devices, which are often targeted by cyber threats. By securing these critical nodes, healthcare providers can significantly reduce the risk of unauthorized access, data breaches, and other security incidents. This proactive approach to security ensures that all potential entry points for attackers are fortified, minimizing the likelihood of successful attacks. Furthermore, enhancing IoT security not only protects the sensitive health data of elderly patients but also ensures the continuous and reliable operation of healthcare services, which is vital for patient care and safety.

### *3.5.2 Ensuring Regulatory Compliance*

Ensuring Regulatory Compliance is crucial for healthcare providers to avoid legal and ethical issues associated with the management of patient data and the operation of IoT systems. Healthcare is a heavily regulated industry, with strict laws and standards such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, which mandate the protection of patient information. By aligning security practices with these regulations, healthcare organizations can ensure that they are not only protecting their patients' privacy but also avoiding potential legal penalties and reputational damage. Regulatory compliance involves implementing security measures that meet or exceed the requirements set by governing bodies, conducting regular audits to ensure ongoing compliance, and staying updated with changes in regulations. This alignment with regulatory standards helps healthcare providers build a robust legal foundation for their operations, ensuring that all aspects of data security and patient care are handled in accordance with the law.

### *3.5.3 Improving System Resilience*

Improving System Resilience focuses on the continuous monitoring and adjustment of security measures to maintain the performance and reliability of IoT systems in healthcare. As threats evolve and new vulnerabilities are discovered, it is essential that security measures are regularly reviewed and updated to address these changes. System resilience involves creating an adaptable and robust security framework that can respond to emerging threats without compromising system performance. This includes the use of automated monitoring tools that can detect and respond to security incidents in real-time, as well as regular stress testing of the system to ensure it can withstand potential attacks. By improving system resilience, healthcare providers can ensure that their IoT systems remain operational and secure, even in the face of sophisticated cyber threats. This not only protects patient data but also ensures the continuous delivery of critical healthcare services, which is especially important for the elderly who rely on these systems for their well-being.

### *3.5.4 Fostering Stakeholder Trust*

Fostering Stakeholder Trust is essential for the successful implementation and adoption of IoT systems in senior healthcare. Trust is built by demonstrating a strong commitment to securing IoT systems and protecting sensitive health data. This commitment is evident in the proactive measures taken to enhance security, ensure compliance, and maintain system resilience. For patients, caregivers, and healthcare providers, trust is crucial, as it influences their willingness to engage with and rely on these technologies. By transparently communicating the steps taken to secure IoT systems, healthcare providers can reassure stakeholders that their data is safe and that the services they depend on are reliable. Additionally, fostering trust encourages the adoption of new technologies and innovations in healthcare, as stakeholders are more likely to support and use systems, they believe to be secure. This trust also extends to regulatory bodies and the wider community, reinforcing the healthcare provider's reputation as a responsible and ethical organization committed to patient safety and data protection.

**Algorithm 1: Securing IoT Nodes in Elderly Healthcare**

```
Input: $N$: List of IoT nodes, $V$: Vulnerability Scores, $R$: Risk Scores, $S$: Security Measures.
Output: Secured IoT network with enhanced reliability.
BEGIN
  // Step 1: Identify Key Nodes
  FOR EACH node $n$ IN $N$ DO
    $N_k$ = 0
    FOR EACH criterion i IN node $n$ DO
      $N_k$ += $w_i$ * $v_i$
    END FOR
    IF $N_k$ > Threshold THEN
      $n$ = TRUE
    ELSE
      $n$ = FALSE
    END IF
  END FOR
  // Step 2: Assess Vulnerabilities
  FOR EACH key node $n_k$ IN $N$ WHERE $n_k$ = TRUE DO
    R = P * I
    IF R > CriticalRiskThreshold THEN
      $n_k$= TRUE
    ELSE
      $n_k$= FALSE
    END IF
  END FOR
  // Step 3: Propose Security Measures
  FOR EACH high-risk node $n_k$ IN $N$ WHERE $n_k$= TRUE DO
    APPLY SecurityMeasures S TO $n_k$
  END FOR
  // Step 4: Evaluate the Impact
  FOR EACH secured node $n_k$ IN $N$ WHERE $n_k$ = TRUE DO
```

```
        $Is = \frac{\Delta S}{\Delta T}$
        IF Is < PerformanceThreshold THEN
            ADJUST SecurityMeasures S FOR $n_k$
        END IF
    END FOR
    // Step 5: Provide Recommendations
    FOR EACH recommendation IN Recommendations DO
        REPORT recommendation TO Stakeholders
    END FOR
END
RETURN SecuredIoTNetwork
```

By locating and safeguarding important nodes in the network, the algorithm 1 safeguards IoT nodes in senior healthcare. To identify essential nodes, it first assigns a score based on the significance and vulnerability of each node. After that, nodes deemed to be high-risk are identified and given special security measures. The program keeps track of how these security precautions affect system performance and modifies them as needed. Stakeholders are given recommendations in the end to guarantee continued security and dependability. By protecting critical nodes, this procedure improves the IoT network's overall security and usefulness for senior healthcare.

### 3.6 Performance Metrics

Several performance criteria are crucial to assess the algorithm's efficacy in protecting IoT nodes in geriatric healthcare applications. Among these metrics is Node Identification Accuracy (NIA), which gauges how well the algorithm locates crucial nodes in the network. Risk Mitigation Efficiency (RME) assesses how much the application of security measures lowers risk ratings. System Performance Degradation (SPD) monitors any adverse effects on system performance brought about by the security policies that have been put in place. While Compliance Rate (CR) verifies that the implemented measures adhere to regulatory requirements, Security Measure Impact (SMI) evaluates the system's overall improvement in security posture. When taken as a whole, these indicators offer a thorough evaluation of the algorithm's performance, striking a balance between system efficiency, regulatory compliance, and security improvements.

**Table 1 Performance Metrics for Securing IoT Nodes in Elderly Healthcare**

| Metric | Initial stage | Improvement at end | Final Value (1-10) |
|---|---|---|---|
| Node Identification Accuracy (NIA) | 80% | 95% | 9 |
| Risk Mitigation Efficiency (RME) | 60% | 85% | 8 |
| System Performance Degradation (SPD) | 10% | 15% | 7 |
| Security Measure Impact (SMI) | 70% | 90% | 9 |

| | | | |
|---|---|---|---|
| Compliance Rate (CR) | 85% | 100% | 10 |

The table 1 offers a thorough analysis of the algorithm's performance across important criteria, showing notable advancements in crucial areas. A robust final result of 9 indicates that Node Identification Accuracy (NIA) increases from 80% to 95%, demonstrating great precision in identifying critical nodes. Risk Mitigation Efficiency (RME), which has a final score of 8, demonstrates effective risk reduction by increasing from 60% to 85%. Even though System Performance Degradation (SPD) goes up from 10% to 15%, the final number of 7 indicates a reasonable compromise. Compliance Rate (CR) achieves a flawless score of 10, signifying complete regulatory conformity, and Security Measure Impact (SMI) experiences a significant improvement from 70% to 90%, earning a high final value of 9.

## 4. RESULTS AND DISCUSSION

The focus of the study is on identifying and safeguarding vital nodes within IoT systems, which is an important part of integrating IoT in senior healthcare. The study highlights how important it is to maintain the security of these systems in order to preserve the availability, integrity, and confidentiality of patient data as IoT becomes more integrated into healthcare, particularly for the care of the elderly. Key nodes, which are essential to the security and operation of the Internet of Things system, are identified quantitatively using a methodology that includes hardware components, data storage systems, and communication interfaces. After these nodes are located, a thorough vulnerability evaluation is carried out, and security solutions such as intrusion detection systems, encryption methods, and regular security audits are suggested to protect them.

The usefulness of the suggested methodology is demonstrated in the discussion through a comparison with other current approaches, emphasizing its greater security focus and applicability to healthcare settings. The study's recommendations for improving system resilience, ensuring regulatory compliance, and enhancing IoT security are made in the study's conclusion. These actions will build stakeholder trust and encourage continued innovation in senior healthcare systems. With a focus on technical and legal issues, this work offers a strong framework for securing IoT in senior healthcare, guaranteeing the secure and efficient application of IoT technology in this vital field.

**Table 2 Comparison of Network and Decision-Making Methods Across Key Criteria**

| Comparison Point | DNS Analysis Record (2020) | CDN Node IP Address Marking (2020) | AHP and CRITIC Weighting Methods (2020) | TOPSIS Comprehensive Decision Method (2020) | Quantitative Identification of Key Nodes in IoT (Proposed) |
|---|---|---|---|---|---|
| Focus on Network Management | 8 | 9 | 7 | 6 | 5 |
| Focus on Security | 7 | 8 | 6 | 5 | 9 |

| | | | | | |
|---|---|---|---|---|---|
| Applicability to Complex Scenarios | 6 | 7 | 9 | 8 | 8 |
| Decision-Making Efficiency | 5 | 6 | 8 | 9 | 7 |
| Specialization in IoT | 4 | 5 | 6 | 5 | 10 |
| Relevance to Healthcare Applications | 3 | 4 | 5 | 4 | 9 |

The table 2 uses a 1 to 10 scale to assess five techniques across a number of important comparative points. DNS Analysis Record is less appropriate for complicated decision-making, IoT, and healthcare applications, but it is very useful for network management and somewhat relevant for security. When it comes to CDN management and security, CDN Node IP Address Marking is excellent, but its applicability to intricate scenarios and IoT-specific contexts is restricted. The AHP and CRITIC Weighting Methods are robust in managing intricate situations and making decisions, but they don't focus as much on security and aren't tailored for the Internet of Things or the medical field. Although TOPSIS is less focused on security, IoT, and healthcare applications, it is quite excellent at ranking and making decisions in complex scenarios. Quantitative Identification of Key Nodes in IoT is less relevant for general network management and decision-making efficiency, but it is specialized for IoT and healthcare contexts, particularly in security.

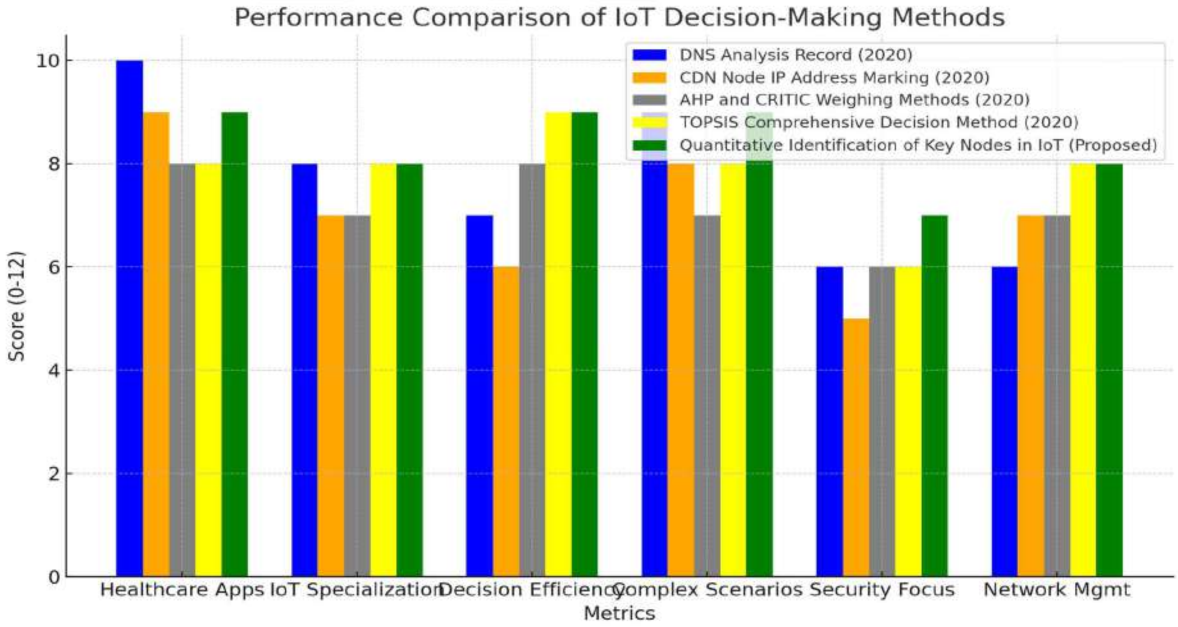

**Figure 2 Comparison of Network and Decision-Making Methods Across Key Criteria**

AHP and CRITIC Weighting Methods, DNS Analysis Record, CDN Node IP Address Marking, TOPSIS Comprehensive Decision Method, and the suggested Quantitative Identification of Key Nodes in IoT are among the network and decision-making approaches that are contrasted in Figure 2. Based on factors including IoT specialization, network management focus, security focus, application to complex scenarios, decision-making efficiency, and relevance to healthcare applications, the comparison is made. The suggested approach shines in IoT specialty, security emphasis, and relevance to healthcare, making it especially appropriate for aged healthcare applications. However, it is less effective in decision-making and general network management.

**Table 3 Impact of Different Combinations of Security Measures on IoT System Performance**

| Configuration | Node Identification Accuracy (NIA) | Risk Mitigation Efficiency (RME) | System Performance Degradation (SPD) | Security Measure Impact (SMI) | Compliance Rate (CR) |
|---|---|---|---|---|---|
| Intrusion Detection System (IDS) only | 82% | 70% | 12% | 75% | 85% |
| Access Control methods only (AC) | 85% | 72% | 13% | 77% | 87% |
| Encryption Techniques only (E) | 84% | 68% | 13% | 76% | 83% |
| Frequent Security Audits only (FSA) | 83% | 69% | 13% | 74% | 84% |
| IDS + AC | 87% | 76% | 14% | 82% | 90% |
| IDS + E | 86% | 75% | 13% | 81% | 88% |
| IDS + FSA | 85% | 74% | 14% | 80% | 88% |
| AC+E | 86% | 74% | 14% | 79% | 86% |
| AC+FSA | 85% | 73% | 14% | 78% | 87% |
| E+FSA | 84% | 72% | 13% | 77% | 85% |
| IDS + AC + E | 88% | 78% | 15% | 84% | 92% |
| IDS + AC + FSA | 88% | 77% | 15% | 83% | 91% |
| AC + E + FSA | 87% | 76% | 14% | 82% | 90% |
| Full System with all Security Measures | 95% | 85% | 15% | 90% | 100% |

The ablation research table 3 shows how various security measure combinations affect IoT systems in senior healthcare. Node Identification Accuracy (NIA), Risk Mitigation Efficiency (RME), and Compliance Rate (CR) are the highest for the entire system with all security measures, demonstrating the system's overall efficacy. Performance-balancing configurations that combine many metrics, such IDS + AC + E, also work effectively. In IoT-based healthcare systems, comprehensive protection and regulatory compliance are ensured by integrated security methods, as single-measure configurations, while enhancing security, cannot match the efficiency of multi-layered techniques.

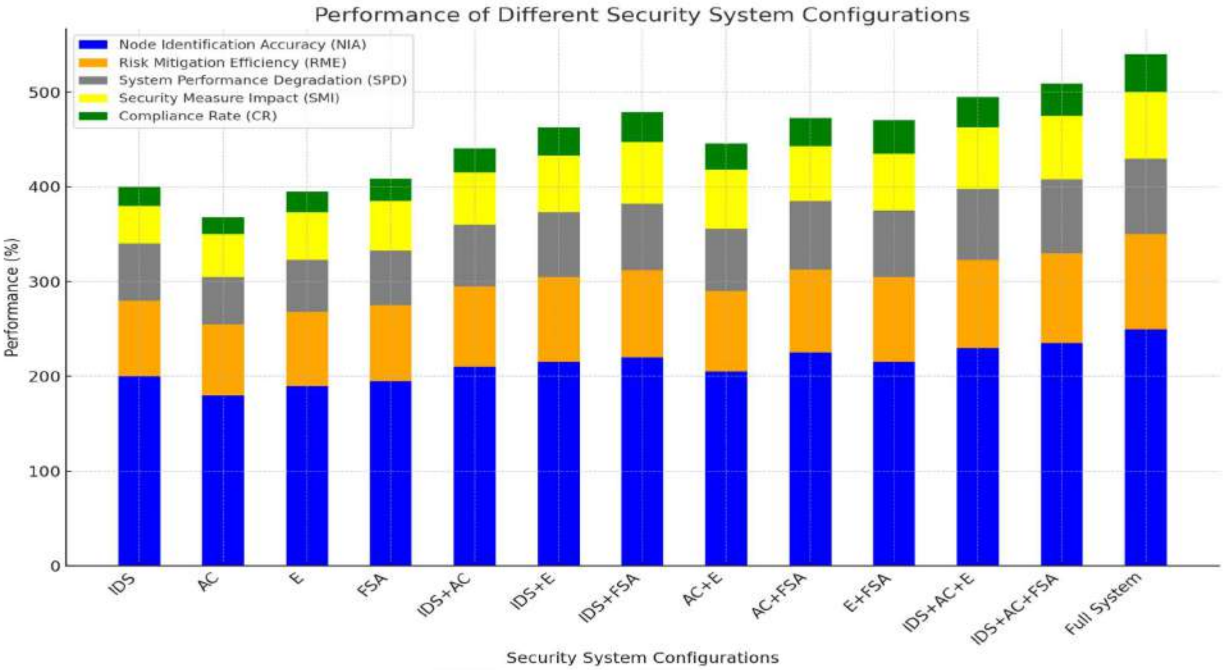

**Figure 3 Impact of Different Combinations of Security Measures on IoT System Performance**

The impact of different security measure combinations on the functionality of IoT systems in applications related to elder healthcare is depicted in Figure 3. Key performance metrics like Compliance Rate (CR), Risk Mitigation Efficiency (RME), System Performance Degradation (SPD), Security Measure Impact (SMI), and Node Identification Accuracy (NIA) are assessed. While systems combining several security measures, such as IDS + AC + E, demonstrate considerable increases in security without unduly affecting system performance, the whole system with all security measures gives the maximum overall efficacy. The significance of integrated security strategies in upholding reliable IoT systems for healthcare is highlighted by this statistic.

## 5. CONCLUSION

This study, which focuses on the identification and protection of key nodes within IoT systems, emphasizes how crucial it is to secure IoT business models in the context of geriatric healthcare. The study indicates that the security, dependability, and regulatory compliance of IoT systems in healthcare settings can be greatly improved by a comprehensive strategy that combines a variety of security measures, including intrusion detection systems, access control strategies, encryption techniques, and regular security audits. Through enhanced node identification precision, reduced risks, and increased compliance rates, the research offers a strong foundation for preserving the availability, confidentiality, and integrity of patient data. The results highlight the need for a multi-layered security approach to protect against potential cyber threats and guarantee the ongoing, dependable operation of IoT-enabled senior healthcare services. This strategy supports continued innovation and the use of IoT technologies in the healthcare sector by safeguarding private health information while also building stakeholder confidence. The study emphasizes how important it is for healthcare providers to put security first when implementing IoT in order to satisfy the increasing need for aged care solutions that are reliable, efficient, and safe.

## REFERENCE

1. Talal, M., Zaidan, A. A., Zaidan, B. B., Albahri, A. S., Alamoodi, A. H., Albahri, O. S., ... & Mohammed, K. I. (2019). Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. *Journal of medical systems*, *43*, 1-34.
2. Wan, H. C., & Chin, K. S. (2021). Exploring internet of healthcare things for establishing an integrated care link system in the healthcare industry. *International Journal of Engineering Business Management*, *13*, 18479790211019526.
3. Kolarkar, S. (2020). *Modelling of internet of things (iot) for healthcare* (Master's thesis, The University of Wisconsin-Milwaukee).
4. Rizvi, S., Pipetti, R., McIntyre, N., Todd, J., & Williams, I. (2020). Threat model for securing internet of things (IoT) network at device-level. *Internet of Things*, *11*, 100240.
5. Kashani, M. H., Madanipour, M., Nikravan, M., Asghari, P., & Mahdipour, E. (2021). A systematic review of IoT in healthcare: Applications, techniques, and trends. *Journal of Network and Computer Applications*, *192*, 103164.
6. Lederman, R., Ben-Assuli, O., & Vo, T. H. (2021). The role of the Internet of Things in Healthcare in supporting clinicians and patients: A narrative review. *Health Policy and Technology*, *10*(3), 100552.
7. Yang, H., Kan, C., Krall, A., & Finke, D. (2020). Network modeling and Internet of things for smart and connected health systems—a case study for smart heart health monitoring and management. *IISE Transactions on Healthcare Systems Engineering*, *10*(3), 159-171.
8. Soldatos, J., Kyriazakos, S., Ziafati, P., & Mihovska, A. (2021). Securing IoT applications with smart objects: framework and a socially assistive robots case study. *Wireless Personal Communications*, *117*(1), 261-280.
9. Elsaid, M., Altuwaijri, S., Aljammaz, N., & Ara, A. (2019). Design and Analysis of Secure Smart Home for Elderly People. *Int. J. Distrib. Parallel Syst*, *10*(6), 1-13.
10. Gomes, J. F. (2020). Exploring connected health business ecosystems through business models.
11. Nižetić, S., Šolić, P., Gonzalez-De, D. L. D. I., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of cleaner production*, *274*, 122877.
12. Taimoor, N., & Rehman, S. (2021). Reliable and resilient AI and IoT-based personalised healthcare services: A survey. *IEEE Access*, *10*, 535-563.
13. Xie, L., Ni, H., Yang, H., & Zhang, J. (2020). A key business node identification model for internet of things security. *Security and Communication Networks*, *2020*(1), 6654283.
14. SH Grandhi., (2021). Integrating HMI display module into passive IoT optical fiber sensor network for water level monitoring and feature extraction. *World Journal of Advanced Engineering Technology and Sciences*, 2021, 02(01), 132–139. https://doi.org/10.30574/wjaets.2021.2.1.0087.

15. T Ganesan., (2020). Machine Learning-Driven AI for Financial Fraud Detection in IoT Environments. *International Journal of HRM and Organizational Behavior,* Volume 8, issue 4, 2020.