Cybersecurity and Compliance in Healthcare: A Study on Key Management and Other Regulatory Requirements

Priya Vij[1], Patil Manisha Prashant[2]

[1]*Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India*
[2]*Research Scholar, Department of CS & IT, Kalinga University, Raipur, India.*

KEYWORDS

Cyber Security, Health, Security, Privacy

ABSTRACT

Typically, WSNs are implemented in several applications with various topologies. Nodes use wireless mode of communication, and unattended areas are typically selected for WSN deployment. Attack risk is higher in WSNs. Furthermore, the WSN nodes have severe resource constraints. It is quite difficult to provide security in such a setting. Numerous protocols for key management chores and encryption strategies for maintaining security in the WSN environment have been documented in literature. The criticality of the data being transferred over the network determines how complex the assault will be. Applications that monitor agriculture, for example, are safe from attacks. However, applications related to the military and healthcare could attract attackers who are far more skilled. Applications that involve process control and habitat monitoring attract attackers with medium to low skill levels. There isn't a single protocol available right now that could be flexible enough to meet the different requirements of the apps, which typically have variable security requirements. For these different applications, there are differences in the key management task, which is strongly related to the security requirements. As a result, the precise kind and complexity of the key management technique must be chosen and built in accordance with the necessary level of security, the capabilities of the hardware devices available, and the network topology that is used.

1. Introduction

The field of patient safety has grown in importance as a result of the growing complexity of healthcare systems and the rising rate of patient injuries in healthcare facilities. Its fundamental objective is to prevent and reduce risks, errors, and harm that patients may suffer when obtaining healthcare services. Fundamental to this discipline is the concept of continuous development, which is reached by a thorough understanding of errors and unfortunate events [1]. The significance of patient safety cannot be overstated, since it is an essential element in delivering essential healthcare services of high calibre. The significance of patient safety cannot be overstated, since it is an essential element in delivering essential healthcare services of high calibre. The global consensus is that the most important factors in providing effective healthcare should be safety, efficacy, and patient-centeredness. To fully benefit from high-quality healthcare, timely, egalitarian, integrated, and efficient services are also required [2]. The effective implementation of patient safety measures requires the cooperation of several crucial elements. It is imperative that healthcare institutions adopt unambiguous rules that prioritise patient safety [3]. Promoting the acceptance and use of patient safety measures requires strong leadership skills. Finding problem areas and enabling safety improvements require data accessibility [6]. Skilled healthcare workers are essential to provide safe and effective treatment to patients [12].

Finally, in order to ensure comprehensive and individualised safety precautions, it is imperative that patients actively participate in their care. Insufficient mechanisms create an environment that increases the likelihood of errors or the incapacity to prevent them, resulting in adverse consequences [4]. Healthcare has been categorised as a "high-hazard industry" due to the inherent risks of disease and death. The developments in the field of medical electronics have led to an increase in the popularity of medical sensing. Numerous locations, including residences, workplaces, hospitals, and living quarters, are using it [5]. In the medical industry, sensors are used to track a variety of indicators, such as heart rate and physical activity. The sensors can also be worn outside the body to monitor the human body's exterior organs. Wearable sensors provide a practical way for warriors to track their actions on the front lines of battle, for patients receiving chronic illness treatment to measure their progress in rehabilitation, and for athletes to track their activity [9]. With the use of key management techniques, secure associations in the form of security keys can be created between the communication nodes. A number of tasks are included in key management, such as the creation, sharing, storing, using, and replacing of security keys. Keys fall into two general categories: symmetric and asymmetric. In the former type, both parties to the communication share the same key, meaning that it is used for both

encryption and decryption. It is necessary to distribute, infer, and store symmetric keys securely. Conversely, in the asymmetric category, two separate but related keys are employed.

2. Methodology

When using basic cryptographic approaches, key generation and its subsequent exchange result in significant energy usage and communication overhead. Advances in technology have led to the development of multiple cryptographic protocols for the production and agreement of keys. Each of these technologies has advantages and disadvantages of its own, and they all respond differently depending on the situation. Therefore, it is necessary to create a particular protocol that may be adjusted to various situations [11]. Three key generation strategies were developed for the proposed research, which allows the sender to encrypt data and send it securely to the recipient [7].

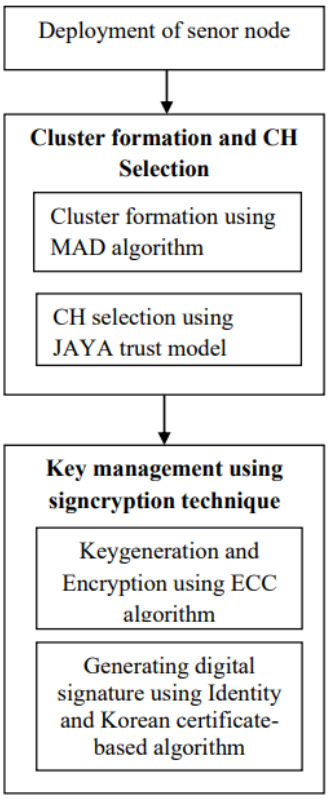

Figure 1. Proposed overflow

This section provides an effective approach for key management that is centred on The Optimal Cluster Based Key Management System (OC-KMS) is advised for heterogeneous wireless sensor networks. It is possible to expand this security architecture for large-scale systems that need complete protection. Sensor node data is gathered by the BS, which then computes the confidence gain (trust value).Based on the trust values, which gather all information from other cluster nodes, BS chooses the CH for each Cluster [8]. The only direct connections that the CHs are eligible for are with the BS and node of neighbouring CHs. Every cluster node has a distinct ID, which is dispersed at random. The method used to transport data between the source and destination nodes is called certificate-less signcryption. The first thing to do is cluster using the Modified Animal Diaspora (MAD) algorithm. The Modified Animal Diaspora (MAD) optimisation algorithm can be divided into two parts: the Diaspora process and the updating process, which determines an appropriate optimal solution [13].

3. Results And Discussion

It is recommended to simulate the key management approach for WSNs using the Network Simulator (NS2) tool. This experiment uses a network with 300, 400, 500, 600, and 700 randomly distributed

sensor nodes dispersed over a 1000 1000 metre region to test various network layer assaults. Each node has a radio transmission range of about 250 meters, and the channel can carry two megabits of data per second. The efficiency of the proposed system (OC-KMS) is evaluated by varying the number of nodes with a defined number attack of 5 and the iteration level of the optimisation algorithm of 100 [10]. Figure 2's delay efficiency for each of the nodes and the delay of the put-forth OC-KMS are clearly visible as being better than those of the current DKMM system, but not as good as they are when considering the increase in node count.

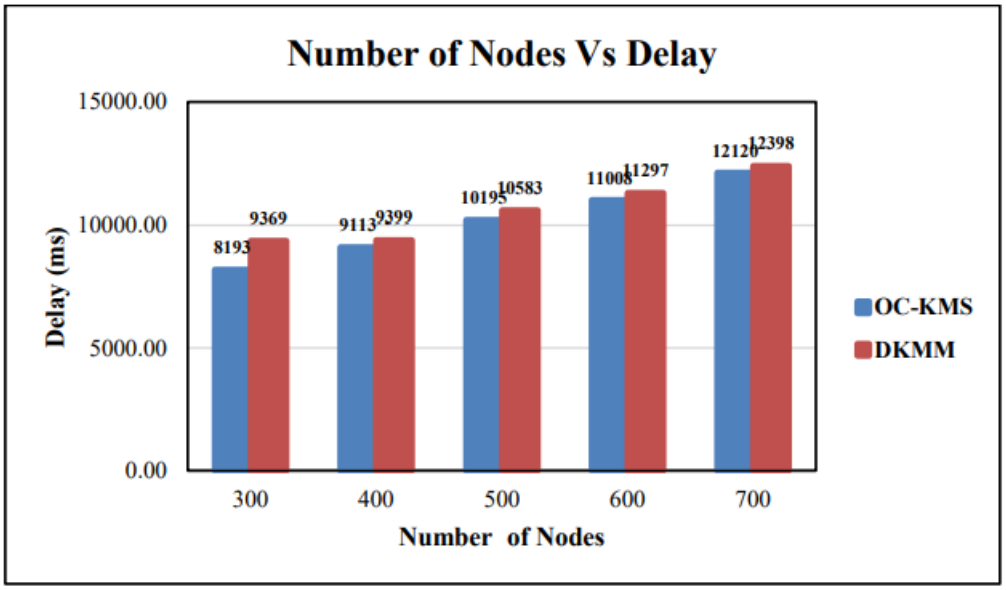

Figure 2. Number of Nodes Vs Delay

The efficiency of the distribution ratio in relation to the different nodes is mapped in Figure 3, where it is evident that the distribution ratio of the proposed OC-KMS is significantly higher than that of the current DKMM system, while slightly lower than the rise in nodes.

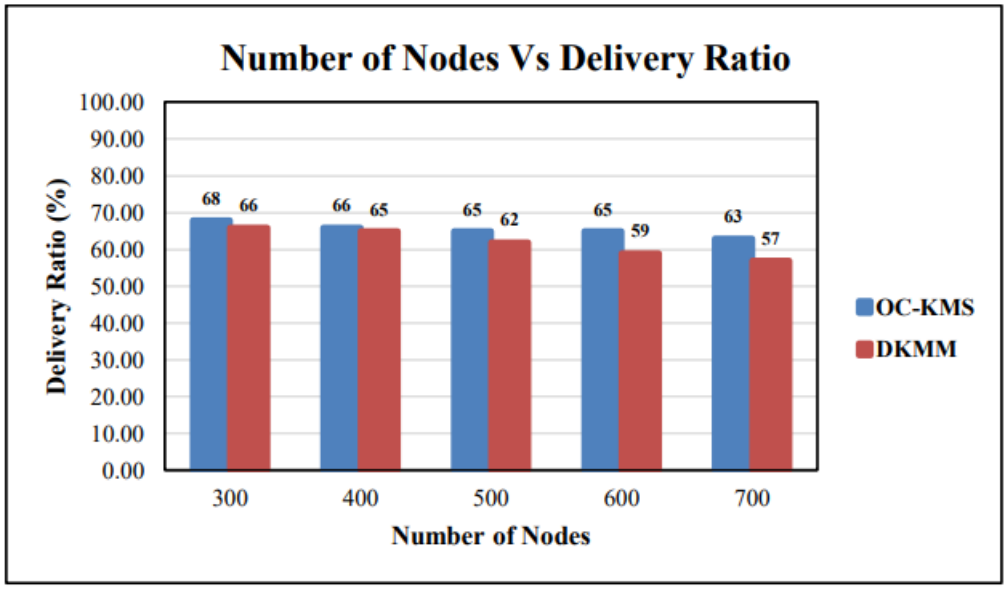

Figure 3. Number of Nodes Vs Delivery Ratio

Figure 4 maps the efficiency of energy consumption with respect to the different nodes. It is evident that the energy consumption of the proposed OC-KMS is significantly lower than that of the present DKMM approach, although it is larger when considering the increase in the number of nodes.

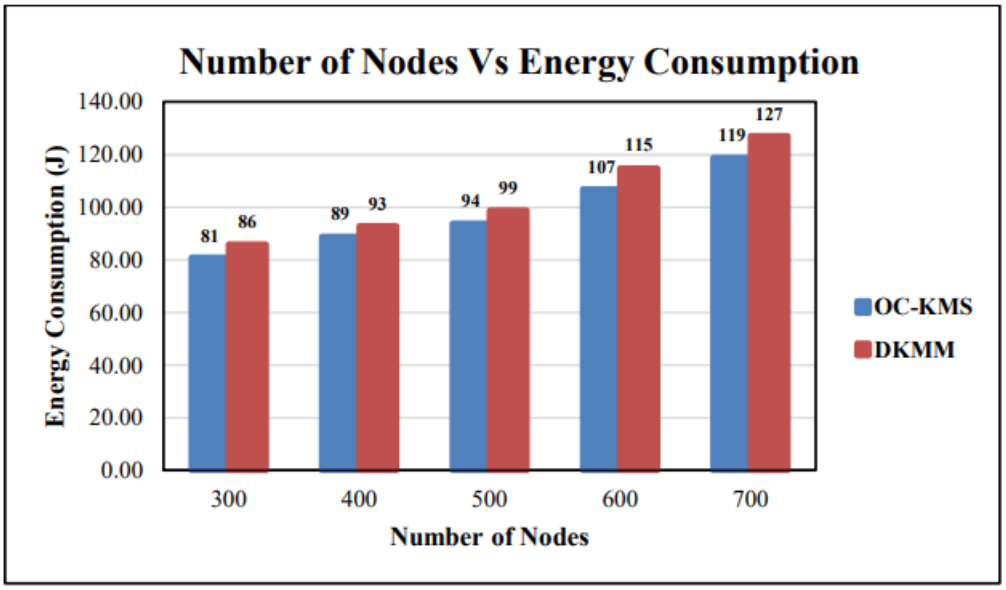

Figure 4. Number of Nodes Vs Energy Consumption

We plot the network lifetime with regard to the various nodes in Figure 5. The network lifetime of the proposed OCKMS is far longer than that of the current DKMM system, and it is accurately represented.

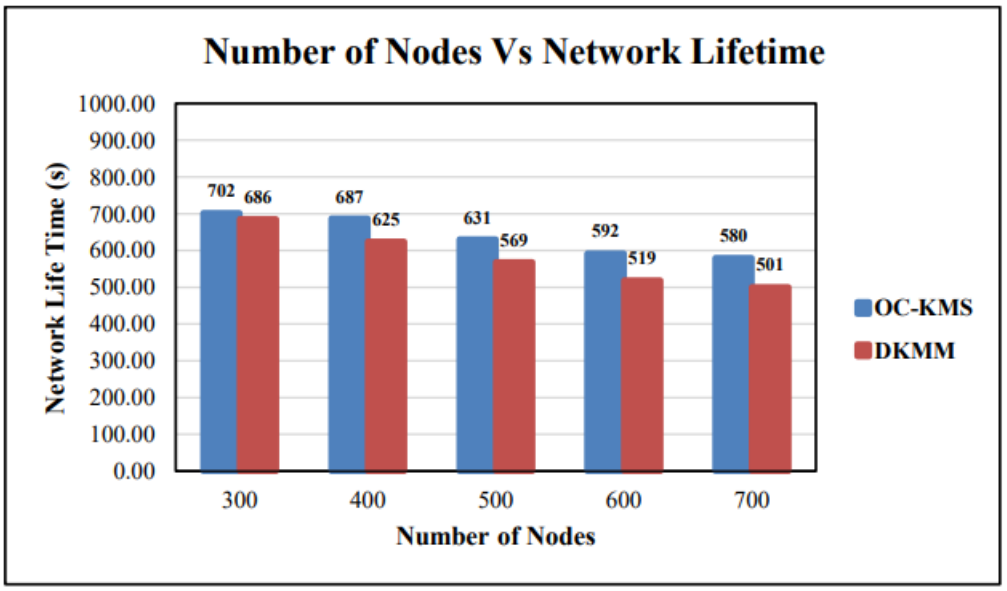

Figure 5. Number of Nodes Vs Network Lifetime

Large-scale applications such as target tracking and surveillance, military, SMART city, health care monitoring, etc. need high security together with support for node mobility. The Modified Animal Diaspora (MAD) optimisation technique and the JAYA trust model, two unique clustering and cluster head (CH) selection models, were provided in the third part of the requested research, which was the design of a security framework.

4. Conclusion

The suggested study focusses on applications that require differing degrees of security and come in a range of sizes. The outcomes of the suggested strategies successfully prevented a number of security assaults, including node capture and jammer attempts. The suggested security measures protect the

devices communicating within the WSN and preserve the privacy, integrity, and confidentiality of the information that is transmitted. The freedom granted to nodes to join and leave the network at any time without warning is one of WSN's primary characteristics. The original method that was put forth used the channel hopping methodology to perform dynamic key generation, which led to a dynamic key update for each conversation that was started over a new channel. Adversaries can simply infiltrate malicious nodes into the WSN and use them to launch a variety of assaults. A jamming attack involves the attacker jamming the transmission path, which causes the data to be transmitted corruptly. The suggested method uses dynamic key management, which causes the data to switch channels while it is being transmitted. As a result, the amount of time data travels across any given channel is decreased. This reduces the likelihood that enemies will mount a successful attack because the transiting channels are constantly shifting.

Reference

[1] Busdicker, Mike, and Priyanka Upendra. "The role of healthcare technology management in facilitating medical device cybersecurity." *Biomedical Instrumentation & Technology* 51, no. s6 (2017): 19-25.
[2] Thomasian, Nicole M., and Eli Y. Adashi. "Cybersecurity in the internet of medical things." Health Policy and Technology 10, no. 3 (2021): 100549.
[3] Sindhusaranya, B., Yamini, R., Manimekalai Dr, M. A. P., & Geetha Dr, K. (2023). Federated Learning and Blockchain-Enabled Privacy-Preserving Healthcare 5.0 System: A Comprehensive Approach to Fraud Prevention and Security in IoMT. Journal of Internet Services and Information Security, 13(3), 199-209.
[4] Marotta, Angelica, and Stuart Madnick. "Cybersecurity as a unifying factor for privacy, compliance and trust: The Haga Hospital case." Issues in Information Systems 23, no. 1 (2022).
[5] Kwon, Juhee, and M. Eric Johnson. "Healthcare security strategies for regulatory compliance and data security." In 2013 46th Hawaii International Conference on System Sciences, pp. 3972-3981. IEEE, 2013.
[6] S. Neelima, Manoj Govindaraj, Dr.K. Subramani, Ahmed ALkhayyat, & Dr. Chippy Mohan. (2024). Factors Influencing Data Utilization and Performance of Health Management Information Systems: A Case Study. Indian Journal of Information Sources and Services, 14(2), 146–152. https://doi.org/10.51983/ijiss-2024.14.2.21
[7] Lee, Chien-Ding, Kevin I-J. Ho, and Wei-Bin Lee. "A novel key management solution for reinforcing compliance with HIPAA privacy/security regulations." IEEE Transactions on Information Technology in Biomedicine 15, no. 4 (2011): 550-556.
[8] Anderson, Scott, and Trish Williams. "Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge?." Computer Standards & Interfaces 56 (2018): 134-143.
[9] Malathi, K., Shruthi, S.N., Madhumitha, N., Sreelakshmi, S., Sathya, U., & Sangeetha, P.M. (2024). Medical Data Integration and Interoperability through Remote Monitoring of Healthcare Devices. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 15(2), 60-72. https://doi.org/10.58346/JOWUA.2024.I2.005
[10] SHAIK, SADULLA. "A coplanar wave guide fed compact antenna for navigational applications." *National Journal Of Antennas and Propagation* 2.1 (2020): 7-12.
[11] Lechner, Nadica Hrgarek. "An overview of cybersecurity regulations and standards for medical device software." In Central European Conference on Information and Intelligent Systems, pp. 237-249. Faculty of Organization and Informatics Varazdin, 2017.
[12] Kelly, Brendan, Conor Quinn, Aonghus Lawlor, Ronan Killeen, and James Burrell. "Cybersecurity in Healthcare." Trends of Artificial Intelligence and Big Data for E-Health (2023): 213-231.
[13] Nifakos, Sokratis, Krishna Chandramouli, Charoula Konstantina Nikolaou, Panagiotis Papachristou, Sabine Koch, Emmanouil Panaousis, and Stefano Bonacina. "Influence of human factors on cyber security within healthcare organisations: A systematic review." Sensors 21, no. 15 (2021): 5119.
[14] Abraham, Chon, Dave Chatterjee, and Ronald R. Sims. "Muddling through cybersecurity: Insights from the US healthcare industry." Business horizons 62, no. 4 (2019): 539-548.