Addressing Privacy and Security Concerns Associated with the Increased Use of IoT Technologies in the US Healthcare Industry

Sumanth Tatineni

Abstract- *The Internet of Things (IoT) enables a wide range of smart devices worldwide to connect to the Internet to ensure they can effectively collect, process and share data. Some of the technologies that have since enhanced the process include IPv6, which ensures that there are no limitations on the number of IP addresses that can be used by every device globally. Most key players in the health sector leverage various IoT devices, which have proven to be a major boost in assisting and monitoring patients remotely. It is the most significant step in the healthcare sector, especially for those living in areas with transportation challenges or even older people residing in remote areas. However, despite the multiple benefits of adopting IoT in the health sector, there are major data security and privacy concerns. Some of the associated risks also include entry points into health organizations' infrastructure and exposure to medical IoT devices, which may eventually undermine the intended objectives of these systems. It is vital to assess some of these concerns, possible solutions and how the end-user environment, the network layer and the cloud layer can all be protected to ensure that they can mitigate the chances of such attacks. It clearly indicates a need to embrace robust security measures and protect all the layers that define the IoT environment.*

Keywords: *IoT, Security risks, Mitigation measures, Privacy, Security threats, Health sector risks.*

1.0 Introduction

The utilization of many IoT devices characterizes today's operational environment in the health sector. The devices range from wearables, monitoring sensors, ingestible, guided imagery, and implantable. All these technologies have played a major role in ensuring that healthcare staff are more informed and able to effectively execute some health-related practices to guarantee better healthcare services and monitoring. This should be seen as a major step in enhancing healthcare services provision. COVID-19 also came in as a major avenue that accelerated the process of adopting IoT in healthcare. Health facilities were becoming more overwhelmed, presenting the need to adopt remote medical consultation. Medical IoT devices are expected to quadruple in the next five years.

IoT in healthcare comprises collecting, processing and transferring vital health data from patients, which makes it attractive to adversaries (Onesimu et al., 2021). Some of the benefits that accrue from the use of IoT technology in the healthcare sector include improved and more personalized patient care. Unfortunately, various medical IoT devices lack robust security. The COVID-19 pandemic was characterized by immense incidences that would make sensitive data inaccessible, with some data even being permanently inaccessible. The health sector turns out to be the most attractive target for adversaries due to the amount of data collected in real time.

Ransomware attacks top the list of some of the most effective techniques adversaries have employed over the past few years (Humayun et al., 2021). The absence of robust and clear techniques to mitigate some of these attacks presents a clear pathway hackers could use to compromise these systems. Additionally, hospitals cannot operate without patient data. As a result, they often give in to hackers' demands by paying ransom every time there is a breach. In multiple instances, hackers have successfully taken over medical devices and made changes that significantly affect the various parameters and configurations that inform medical decisions. All these ripple effects may have fatal consequences on the various medical procedures.

2.0 Overview of IoT in the Healthcare Sector

There is a significant increase in the number of high profiles of cyberattacks targeting major essential services and facilities. The worst part is that as the number also increases, the severity of these attacks increases. According to the World Economic Forum Global Risk Report of 2019, data breaches and cyberattacks were among the top five threats in the modern world. The worrying happening is the repeated attacks that have been consistently targeting healthcare organizations, with the most employed technique used by hackers is ransomware. The targeted attacks on various health infrastructure compromise the whole process of addressing the need of patients.

Healthcare organizations have constantly been at the forefront in embracing efforts to ensure that they adopt techniques and practices that embrace personalization and the highest level of service by leveraging technology. Unfortunately, these same institutions are put under immense pressure due to the multiple issues around the healthcare industry, which seem to be undermining the same efforts these institutions are putting in place. Among the issues currently in the healthcare sector include the increasing concerns around data security, increasing healthcare-related costs, and new and reemerging diseases, among others. All these challenges present the dire need to fully migrate to technology and leverage it to try and address them.

IoT presents an ideal approach for healthcare service providers to access a wide range of patient information. It has also created an avenue for healthcare professionals to offer their services through a contactless approach, an opportunity that has since enhanced clinical outcomes and productivity amongst practitioners. With IoT, it is quite easier to monitor patients remotely. IoT-based solutions are powered by sensors that can relay information through secure channels. IoT also allows for the utilization of advanced algorithms capable of making in-depth analyses which can then be used to make informed and accurate decisions.

There are multiple benefits realized from using some of these devices, considering how effective they are in monitoring several variables in the human body without the physical presence of a medical practitioner (Lawal & Rafsanjani, 2022). All the trends collected from physiological data are often synced with medical practitioners who can be alerted in case of emergencies. IoT-based technology also simplifies the process of running clinical tests due to the advanced data collection mechanisms created by IoT. It has become prevalent that technology would be so hard to avoid due to its immense benefits and how it has become quite significant in every individual’s life. There is also a clear indication that the amount of personal data to be collected will increase significantly. As a result, these major advances point to the importance of cybersecurity, not because of the

constantly increasing number of attacks or adversaries but because of the sensitive nature of data being accumulated by these technologies.

3.0 Related Work

3.1. Security Concerns in IoT Healthcare Systems

According to the Allied Business Intelligence Inc. (ABI) research report, the number of connected IoT devices has surpassed 10 billion, with the anticipation that the number will grow more significantly by 2027 (Attaran, 2023). The heavy investment in IoT and, more specifically, in the health sector paves the way for an immense number of applications that will translate to major improvements in how health practices are executed. The advent of modern health management applications continues to attract more attention among medical practitioners. However, this does not negate the emerging challenges of integrating IoT technologies into the health sector. Some key issues that should remain in the picture include data management techniques, devices used, data transfer mechanisms, privacy, unified access, and security. All instances of cyberattacks can instigate major damage to not just the reputations of key players in the sector but also the individual users or beneficiaries of the technology. Additionally, for all successful breaches, adversaries may have unlimited access to individual users of IoT technology.

Even though IoT in the health sector continues to be the ideal way to go for more effective services, the challenges around security remain. Some of the applications and technologies that are in use and are the most effective today are due to IoT and the major advances that have been made in space. However, the connection and the relationship between healthcare and personal data and concerns around privacy amongst other relevant health information of patients presents a major security concern.

IoT only works if the Internet is leveraged, implying how easy it can be for devices in the ecosystem to be easily breached due to increased exposure. This implies when dealing with these kinds of technology, it is vital to effectively integrate robust security mechanisms, especially in the communications component of IoT infrastructure. The database is also a major concern that should be effectively addressed, considering this is where all the data is stored. The data profiling process is simplified, with the database being employed to support the IoT devices' functionality. The components making up the IoT ecosystem in the healthcare sector present numerous security concerns likely to undermine data integrity, privacy, and confidentiality. Authentication between devices and how information flows between these devices also serve as additional points of concern.

IoT ecosystems in the health sector comprise gateways, sensors, and actuators and are subject to cases of data theft, confidentiality concerns, and data privacy (Waris et al., 2022). Such a context allows adversaries to compromise mechanisms in place, for instance, if it is a home network that lacks recommended security checks. Data profiling also crystallizes in cases where the adversary compromises an ecosystem and mines data intending to use the harvested data to know the targeted person. Adversaries have often employed multiple techniques to execute their data breaches; selective-forwarding attacks, sinkhole attacks, jamming, flooding, and phishing.

Selective-forwarding attacks allow the execution or deployment of Denial of Service (DoS) attacks (Núñez Segura et al., 2019). This attack is characterized by using malicious nodes to forward packets, with the paramount intention being to trigger a disruption of the routing paths in a network. An excellent example is a scenario where an adversary uses this technique to prevent systems from generating alerts when a deployed sensor detects that a patient may have an urgent issue, such as a heart attack, and may require immediate attention.

Sinkhole attacks are often characterized by malicious nodes advertising artificial routing pathss to attract nearby nodes with the main objective of routing all traffic through them. The sinkhole attack is not focused on disrupting normal network operations. However, the consequences become more dire if this attack is used together with selective-forwarding attacks (Zaminkar & Fotohi, 2020). As a result of such attacks, information ends up in the adversaries' computer rather than the legitimate computer within the health organization's computer. Through sinkhole attacks, adversaries can steal highly sensitive information, including the patient's profile.

Jamming is also a common technique used by adversaries and is instigated through machine-to-machine attacks. This form of attack often executes by taking up the wireless spectrum, which translates to full blockage of communication across IoT devices. The outcome of a jamming attack is a noise signal often applied by adversaries looking to interfere with wireless communications.

Flooding is utilized by adversaries making attempts to overpower the target's resources. For instance, flooding drains memory, battery, processor, and bandwidth resources. A common approach that adversaries usually apply is establishing multiple connection requests or geared towards depleting the batteries of the target node and taking up most of the bandwidth. The implications resulting from the successful execution of this attack is the continuous transmission and recording of information, which for the case of the healthcare IoT, could be sensor data.

Phishing is applicable when attackers are looking to steal individual information. The next step usually comes to gathering the data from the rest of the nodes making up a network (Naaz, 2021). A common approach that is prevalent with phishing is that which targets information from specific users, especially those with high-level access. They can easily access the rest of the IoT resources with such information. The various security concerns targeting IoT nodes often undermine their ability to function effectively to a point that can easily spread to the rest of the healthcare IoT ecosystem. It is also one of the main reasons why adopting IoT in large scale may be a challenge. However, multiple solutions can be leveraged to address some of these prevailing concerns.

3.2. IoT Security Solutions

Privacy and security top the list of major concerns in all IoT ecosystems. As a result, it is one of the critical domains that continue to attract multiple scholars intending to establish a clear understanding of the best solutions that should be adopted to address some of these concerns. Gupta et al. (2019) came up with a proposition of how lightweight authentication should be implemented across all wearable devices. The approach would be backed by cryptographic hash functions, which would ensure a robust security framework protecting all forms of communication within a network. The solution, according to Gupta et al. (2019), is the most effective considering

how most of these devices only operate on limited resources. Regular security and privacy solutions may not work effectively since they have not been developed to meet the needs of wearable devices. The suggested approach utilizes XOR and hashes functionality to conceal the wearable devices' identity, thus capable of operating anonymously and guaranteeing privacy preservation.

Gope and Sikdar (2018) proposed adopting a lighter version of the existing two-factor authentication technique as one of the modes that could be used to preserve privacy for IoT devices. Gope and Sikdar (2018) further emphasize the importance of the technique considering the open nature and how public IoT devices operate, an attribute which renders them highly vulnerable and can easily be compromised. The approach leverages one-way hash values. The other approach also utilized by the skim is physically unclonable functions (PUFs) comprising Integrated Circuits (ICs). As a result, they can generate random physical variations, which would constantly make the ICs unique.

The Internet Protocol Version 6 (IPv6) is among the most futuristic technologies focused on ensuring that even the needs of the future generations are accommodated, including the billions of IoT devices that are likely to be onboarded. IPv6 is ideal since it allows for a larger room than its predecessor IPv4 internet protocol. Unfortunately, based on its structure, it is still susceptible to DoS attacks when configuring the IP, a setback that is likely to result in an interruption of communication between nodes within a network. A major proposition by Liu et al. (2020) is a relatively unique model; an Address-less IoT server which is supposed to ensure secure communication between the IoT server and the IoT client. Rehman and Manickam have also developed a less sophisticated mechanism, Secure-DAD, which should be implemented on IPv6-enabled IoT devices when installing them, a technique that would only allow authenticated devices to communicate with them. Through this approach, there will be guaranteed secure communication among all the devices operating in the IoT environment.

Sharma et al. (2018) put out a privacy-preserving model which should be applied for IoT devices, more so those responsible for data mining. The model is geared towards ensuring that there is effective health systems monitoring. Anantharam et al. (2015) through their study has employed kHeatlh as a system focused on conducting monitoring activities and running an in-depth analysis of the various challenges prevalent in the IoT ecosystem accompanied by all the privacy issues.

A proposition by Wang et al. (2018) suggested that the focus should be on the data processing system with the intention of improving network reliability and speed, especially when sharing patient data over any IoT architecture. They recommended the Reduced Sensor Data Processing Framework (REDPF). The concept of the REDPF is fog computing, where the author employed the Reduced Variable Neighborhood Search (RVNS) algorithm. The main purpose of the algorithm was to introduce enhancements to the overall process of transmitting data while also fostering load balancing. The framework was crafted to leverage a self-adaptive filter that can recollect incorrect or missing information autonomously, rendering it a fault-tolerant system.

Srinivas et al. (2018) suggested that the main focus should be cloud-based authentication for IoT users. The system would also work as a monitoring scheme which would allow for the creation of secret session keys to secure all communications between all wearable sensor nodes and authorized users. The authors employed the Real-Or-Random (ROR) model to conduct security analysis to establish whether the model was susceptible to some of the common forms of attacks utilized by adversaries.

Raifa Akkaoui's (2021) proposition was the use of a decentralized authentication scheme. The proposal, which was also ideal for the IoT healthcare system, would be used to minimize the possible impacts of distributed denial of services attacks (DDoS), one form of attack which is most prevalent in IoT environments. The model's approach takes advantage of the various decentralized features prevalent in blockchain technology. The author of the scheme subjected it to multiple tests, among them over the Ethereum platform, to assess its privacy and security analysis. According to Raifa Akkaoui (2021), the model guarantees privacy, anonymity, integrity and confidentiality of IoT devices and their respective users.

4.0 Security Benchmark for IoT Architecture

IoT architecture comprises three main layers; physical, network, and application. Unfortunately, limited security measures address the challenges facing the current IoT setup. Having a clearly defined benchmark for the IoT architecture is vital based on fundamental information and security principles. The benchmark should encompass all the standard security parameters in various IoT systems. It is, essential to highlight all the criteria of IoT system evaluation before they are deployed as solutions in an operational environment. The outcome of each evaluation should then be used in measuring the security posture of the suggested solution designed for the IoT architecture. The higher the score, the more likely chance that the solution will also be more secure.

The existing IoT architecture does not have sufficient security features begging the need to map the three basic layers; physical, network, and application. The physical layer encompasses the IoT-end devices such as actuators, sensors, and wearable devices. This layer takes the position of a subscriber and the publisher in any IoT environment. The network layer comprises routers deployed as gateways and are tasked with transmitting all processed data from IoT end-devices to cloud servers, where there are either stored or subjected to various analytics procedures. Finally, the application layer is where multiple services such as messaging, data analytics, storage and data processing are made available to the IoT users depending on their specific subscriptions.

It is also vital to clearly define the various security characteristics. Authentication will ensure that all IoT devices are recognized and validated before entering a network. All entities should therefore have unique key identifiers. Confidentiality is focused on ensuring that all the information in the IoT ecosystem is protected from unauthorized users. It is also prudent to only store all information securely to avoid exposure to unauthorized entities. Integrity should be maintained to guarantee that all information being relayed across the ecosystem is not subjected to any form of delay alteration.

In cases where nodes encounter any form of failure, self-healing should allow the system to be aware of the environment and ensure that the right actions are taken to restore the entire system to the initial working state while maintaining the recommended security levels. Fault tolerance is vital since it helps during crash instances and the system should keep on working. In cases where certain components fail, it should not result in total failure of the rest of the system. It is also keen to acknowledge that there are failures that can be predicted to ensure that the overall system or the rest of the nodes are not affected. There are instances where multiple nodes or components in an IoT ecosystem may be damaged. It is vital that the system still be able to mitigate any form of attack. Even in cases where there is a complete system failure, there should be mechanisms to ensure that the level of security is not compromised.

Data freshness is vital to guarantee that the data should be up-to-date during every instance when data should be accessed to guarantee effective and accurate data analysis (Jaigirdar et al., 2019). Trust is recognized in data privacy and is geared towards ensuring that it resonates and meets access control needs and identity management. End users must be guaranteed privacy and at no point no information will be leaked or misused. Firewalls should also be well configured to minimize the ports and IPs allowed and instead focus on the necessary services only.

5.0 Possible Solutions to Mitigate Privacy and Security Concerns

The typical IoT ecosystem encompasses a collection of databases, servers, and gateways that operate in both the cloud and gateway servers (Miraz & Ali, 2018). It should also implement the microservices approach implying a modular approach rendering it easy to operate. Other considerations should entail scalability, additional integrations and improvement. The gateway is responsible for handling all aspects of communication with all the devices in the end user's environment. A middleware is ideal for ensuring that it has been effectively put in to handle all the nodes to guarantee seamless functionalities such as subscriptions, notifications, and even interoperability needs. The middleware also serves as a platform for managing all the connected nodes. Setting up an access protocol management module ensures, as outlined by the IEEE standards, is leveraged to guarantee seamless management of the various communication protocols (Deng et al., 2020). The gateway also ensures that there is seamless communication with all the devices connected, which allows the carrying of data over a short distance. The next step involves transmitting the data to the cloud servers over 802.11 IEEE protocol over the Internet. The approach for sending information over to the Internet should be lightweight, a perspective achieved by ensuring small code is used to cater for transmission need and lightening the bandwidth.

Ensuring security will require that data transmission is only done through secured channels, especially if it is taking place from the environmental nodes to the cloud nodes. The channel will also require authentication techniques which should take place from both sides before the connection takes place. Even if a secure channel has been provided, there will still be major challenges with the end-user environment. As a result, there will be a need to ensure that each gateway is still configured with robust firewalls. The firewall will play a vital role in restricting communications, a move that will significantly reduce intrusion risks.

A common challenge prevalent in the IoT ecosystem is data-stealing, actions that usually leverage data profiling to identify the device's owners (Kaushik et al., 2022). This threat can be mitigated by embracing anonymity which should be prefaced by the gateways' address rather than relying only on the users' personal identities. The middle server, responsible for forwarding, should be able to control communications so that it only happens between unique nodes. The node operating from the user's environment should be unique, just as the server node should also be unique. If the communication is not from the unique nodes, it should not be forwarded, but if it is from a unique node, once the information arrives at the unique server, the information relayed can be stored in the database. From the cloud server side, their firewall rules should be applied so that only information or communication from authorized parties can be received. As a result, connections to the cloud servers will remain restricted, with the channels also restricted. All the information gathered by the cloud servers will remain persistent and secure.

An additional secure channel for access will have to be deployed to ensure that all nodes seeking to access the channel are eligible to see the dashboard. However, confidentiality and privacy will still prevail even upon a node getting access to a specific dashboard. The dashboards are only restricted to specific users who will have access to the information. Essentially consolidating the security and all the security agents deployed across all the existing environmental nodes and the cloud servers in such a manner that they will be aware of both environments. If, at any point, intrusions are detected, the intruder will be automatically logged out of the system.

5.1. End-User Environment Layer

The end-user environment encompasses nodes such as gateways, actuators, and sensors. Sensors are concerned with gathering environmental information such as door state, vital signs, and user motion, among others. The gathered information is then sent to the gateway, where it is processed and stored per specific data models. It is a clear implication that the gateway is the only device exposed to the rest of the Internet. However, it can still use the published or subscribed protocol to publish all the collected information using the secure tunnel. As a result, the gateway has to be configured with a robust firewall table that will only disseminate information to the right peer.

5.2. Network Layer

In the network, two servers play a vital role in securing the communication channel over the Internet. The servers also play an accountability role, creating the Secure Socket Layer (SSL) certificates for all the peers making up the cloud infrastructure. This also covers the gateways present in the end-users' environment (Kumar et al., 2020). The network servers also play an important role in ensuring that the tunnels originating from the end-user's environment to the cloud is secure. However, additional propositions should be considered. First, TCP, which has been used for quite some time, may be slower but presents a great deal of reliability, unlike the UDP protocol, which may be fast but does not allow for acknowledgement. Therefore, TCP allows for guaranteed delivery of information to the other side. Virtual Private Networks (VPNs) focus on encryption of the control channel while ensuring that the data channels are encrypted to guarantee reasonable security.

Preventing man-in-the-middle attacks calls for data authentication techniques such as Secure Hash Algorithm (SHA). This mechanism ensures that there is a unique fingerprint for valid TLS certificates which can only be validated through VPN clients. SHA-2 is likely to work better, unlike SHA-1 (Khan et al., 2022). However, normal HTTPS traffic utilizes TCP port 443, which is in turn combined with the VPN server rendering it more challenging to adequately distinguish multiple VPN connections and other connections used by other remote sites such as online banks or email providers. This clearly indicates that the VPN connection may be harder to block. Securing handshakes Elliptic Curve Diffie-Hellman (ECDH) utilized alongside the ECDSA signature guarantees a significantly higher level of secrecy. Additionally, an industry-wide symmetric key cipher, AES, characterized by a 256-it key size, is ideal accompanied by a unique nature of all connections.

5.3. Cloud Layer

The cloud architecture encompasses redundant and scalable architecture. It is recommended to have a single control panel and multiple nodes, all supporting the cloud nodes with the database for the final storage. Only published or subscribed protocols should be utilized to acquire the data relayed from the gateway operating in the end-users environment. Furthermore, it is vital to keep track of the rest of the architecture capable of giving notification when there are errors in the cloud and the environmental nodes.

6.0 Critical Analysis

To achieve reliability while assessing the effectiveness of IoT solutions, evaluation should be done by assessing the security characteristics. The key parameters that should be considered should include the authentication mechanisms, confidentiality levels, data freshness, fault tolerance, trust and resilience. Authentication is the only aspect that guarantees that legitimate users or devices can be part of the IoT healthcare environment (Kavianpour et al., 2022). It is the most essential factor that will guarantee that most of the security issues are adequately addressed, especially when dealing with impersonation attacks. An excellent example is an instance where foreign nodes masquerade as genuine hosts. Confidentiality encompasses protecting sensitive data from unauthorized access thus preventing the chances of modifying attacks and maintaining the overall integrity of the shared data. This is more applicable, especially when operating in public networks.

Resilience is helpful when ensuring that the system is fully available to users, even during malicious incidences. Resilience is helpful, especially when dealing with DoS attacks which are becoming more prevalent in IoT healthcare (Kandah et al., 2019). Data freshness also focuses on ensuring that information remains recent and that at no point would attackers gain access to the network. Through data freshness, it is also possible to mitigate other instances of man-in-the-middle attacks. Fault tolerance capability also ensuress that IoT networks deliver uninterrupted services to all its users regardless of whether there are system failures. Self-healing presents the potentiality of an IoT network to restore the system in cases where errors emerge and may undermine the rest of the system.

7.0 Conclusion

All the components demonstrated in the paper are vital in ensuring that security and privacy in IoT can be achieved if all the components are considered. It should be noted that healthcare applications should not see reliability as an accessory but should be treated as a precondition for health IoT systems to operate effectively. Monitoring will still call for persistence to guarantee that all incoming data are secured, and ways to access them remain secure. If systems fail the terms of security aspects at any point, it would be impossible to guarantee their effectiveness and ability to meet their intended purpose. IoT solutions have advantages and limitations, but integrating interoperable mechanisms will render the ability to provide robust security services for IoT systems across the three layers. The biggest challenge, however, would be that all the schemes may be based on different protocols and may hinder the need to achieve compatibility.

All in all, it is critical to constantly explore multiple schemes that could contribute significantly in mitigating multiple avenues of attacks. The paramount goal should be guided by the need to ensure that all components are scalable and heterogenous. Even though limited features may be leveraged to guarantee security of all the components that make up the IoT ecosystem, a loss will still need to be done to ensure that the criteria are effectively fulfilled.

References

Akkaoui, R. (2021). Blockchain for the management of Internet of Things devices in the medical industry. *IEEE Transactions on Engineering Management*.

Anantharam, P., Banerjee, T., Sheth, A., Thirunarayan, K., Marupudi, S., Sridharan, V., & Forbis, S. G. (2015, June). Knowledge-driven personalized contextual mhealth service for asthma management in children. In *2015 IEEE international conference on mobile services* (pp. 284-291). IEEE.

Attaran, M. (2023). The impact of 5G on the evolution of intelligent automation and industry digitization. *Journal of ambient intelligence and humanized computing*, *14*(5), 5977-5993.

Deng, C., Fang, X., Han, X., Wang, X., Yan, L., He, R., ... & Guo, Y. (2020). IEEE 802.11 be Wi-Fi 7: New challenges and opportunities. *IEEE Communications Surveys & Tutorials*, *22*(4), 2136-2166.

Gope, P., & Sikdar, B. (2018). Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. *IEEE Internet of Things Journal*, *6*(1), 580-589.

Gupta, A., Tripathi, M., Shaikh, T. J., & Sharma, A. (2019). A lightweight anonymous user authentication and key establishment scheme for wearable devices. *Computer Networks*, *149*, 29-42.

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), 105-117.

Jaigirdar, F. T., Rudolph, C., & Bain, C. (2019, January). Can I trust the data I see? A Physician's concern on medical data in IoT health architectures. In *Proceedings of the Australasian computer science week multiconference* (pp. 1-10).

Kandah, F., Cancelleri, J., Reising, D., Altarawneh, A., & Skjellum, A. (2019, July). A hardware-software codesign approach to identity, trust, and resilience for iot/cps at scale. In *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 1125-1134). IEEE.

Kaushik, S., Bhardwaj, A., Alomari, A., Bharany, S., Alsirhani, A., & Mujib Alshahrani, M. (2022). Efficient, lightweight cyber intrusion detection system for IoT ecosystems using mi2g algorithm. *Computers*, *11*(10), 142.

Kavianpour, S., Shanmugam, B., Azam, S., Zamani, M., Narayana Samy, G., & De Boer, F. (2019). A systematic literature review of authentication in Internet of Things for heterogeneous devices. *Journal of Computer Networks and Communications*, *2019*.

Khan, B. U. I., Olanrewaju, R. F., Morshidi, M. A., Mir, R. N., Kiah, M. L. B. M., & Khan, A. M. (2022). Evolution and analysis of secured hash algorithm (SHA) family. *Malaysian Journal of Computer Science*, *35*(3), 179-200.

Kumar, V. V., Devi, M., Raja, P. V., Kanmani, P., Priya, V., Sudhakar, S., & Sujatha, K. (2020). Design of peer-to-peer protocol with sensible and secure IoT communication for future internet architecture. *Microprocessors and Microsystems*, *78*, 103216.

Lawal, K., & Rafsanjani, H. N. (2022). Trends, benefits, risks, and challenges of IoT implementation in residential and commercial buildings. *Energy and Built Environment*, *3*(3), 251-266.

Liu, R., Weng, Z., Hao, S., Chang, D., Bao, C., & Li, X. (2020). Addressless: enhancing IoT server security using IPv6. *IEEE Access*, *8*, 90294-90315.

Miraz, M. H., & Ali, M. (2018). Blockchain enabled enhanced IoT ecosystem security. In *Emerging Technologies in Computing: First International Conference, iCETiC 2018, London, UK, August 23–24, 2018, Proceedings 1* (pp. 38-46). Springer International Publishing.

Naaz, S. (2021). Detection of phishing in Internet of things using machine learning approach. *International Journal of Digital Crime and Forensics (IJDCF)*, *13*(2), 1-15.

Núñez Segura, G. A., Margi, C. B., & Chorti, A. (2019). Understanding the performance of software defined wireless sensor networks under denial of service attack. *Open Journal of Internet Of Things (OJIOT)*, *5*(1), 58-68.

Onesimu, J. A., Karthikeyan, J., & Sei, Y. (2021). An efficient clustering-based anonymization scheme for privacy-preserving data collection in IoT based healthcare services. *Peer-to-Peer Networking and Applications*, *14*, 1629-1649.

Rehman, S. U., & Manickam, S. (2016). Denial of service attack in IPv6 duplicate address detection process. *International Journal of Advanced Computer Science and Applications*, *7*(6).

Rehman, S. U., & Manickam, S. (2017). Improved mechanism to prevent denial of service attack in IPv6 duplicate address detection process. *International Journal of Advanced Computer Science and Applications*, *8*(2).

Sharma, S., Chen, K., & Sheth, A. (2018). Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. *IEEE Internet Computing*, *22*(2), 42-51.

Srinivas, J., Das, A. K., Kumar, N., & Rodrigues, J. J. (2018). Cloud centric authentication for wearable healthcare monitoring system. *IEEE Transactions on Dependable and Secure Computing*, *17*(5), 942-956.

Wang, K., Shao, Y., Xie, L., Wu, J., & Guo, S. (2018). Adaptive and fault-tolerant data processing in healthcare IoT based on fog computing. *IEEE transactions on network science and engineering*, *7*(1), 263-273.

Waris, Z., Jaleel, A., Shoaib, M., Nigar, N., & Abalo, D. (2022). A Suite of Design Quality Metrics for Internet of Things by Modelling Its Ecosystem as a Schema Graph. *Mathematical Problems in Engineering*, *2022*.

Zaminkar, M., & Fotohi, R. (2020). SoS-RPL: securing Internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism. *Wireless Personal Communications*, *114*(2), 1287-1312.