Intelligent Cyber security Standard for the Healthcare Sector using Internet of Things.

T.Kuppuraj[1*]

[1]Research Scholar in Computer Science, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore – 21

TKuppuraj66666@outlook.com

M.Mohan Kumar[2]

[2]Associate Professor, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore – 21

MMohanKumar452@outlook.com

Abstract:

A recent technological development is the Internet of Things (IoT) that has already had a profound effect on the worldwide network of computers, mobile phones, smart appliances, smart items, data, and information. IoT is a rapidly developing field that offers a wide variety of intelligent solutions and applications. Electronic solutions span the gamut, from transportation to healthcare to smart homes and factories. With the prevalence of cyberattacks, security has risen to the forefront as a top priority for IoT implementations. Since many devices are being added to the IoT, which means more and more of them are online and open to potential attacks, where the security has become a big challenge. There can be no progress in the IoT without first ensuring the safety of its various components. Preserving and integrating disparate Information Communication & Technology (ICT) and smart devices are central to this paradigm. Therefore in this paper propose a framework known as Intelligent Cybersecurity Standard for the Healthcare Sector [ICS-HS] to mitigate the challenges raised above in the medical sector. The future importance of Smart Healthcare applications has been further emphasized by the pandemic. This work analyzes the security threats, latency rate, performance, effectiveness and prediction of the smart health devices and recommends solutions for mitigating them.

Keywords: Cyber Security, Healthcare, Smart devices, IoT, Safety

1. An Overview of IoT Healthcare Environment:

The IoT refers to a system in which many types of connected physical items exchange data with one another [1]. Increased IoT adoption is visible throughout industries, and it has helped to bridge the gap between Information Technology (IT) and IoT [2]. It is a technology that's been growing at a quick rate recently all around the world where many cyber-security tools rely on IoT infrastructure. Several sectors, including the military, education, finance, healthcare, industry, and transportation, can benefit from it [3]. In the next few years, the IoT market and the Internet will grow to accommodate roughly 50 billion linked devices [4]. It is compatible with many kinds of networked devices that can monitor, gather, and process data before uploading it to a private or public cloud [5]. IoT systems are already present in every aspect of human life, including athletics, classrooms, stores, public works, transportation networks, and healthcare [6].

The IoT is a complex concept that has been growing and changing ever since it is first introduced [7]. The IoT is essentially a system in which digital and analog machines and computer devices are given unique identifiers (UIDs) and the capability of exchanging data with one another automatically, without the need for personal communication [8]. This often involves a user communicating with a central device or software, such as a

smartphone app, which then relays the user's information and commands to other, less central, IoT devices [9]. Devices in the periphery can perform necessary tasks and relay information to a central computer or program [10].

As a rule, this entails a human being connecting with a hub device or application, typically a mobile app, which then communicates with and controls a group of peripheral IoT devices [11]. The peripheral devices can perform necessary tasks and relay information to the central device or app, where it can be accessed by the user [12]. Interactions between patients, healthcare providers, and other technology can have a significant impact on the quality of care provided by medical devices [13]. Networks that improve communication, safety, and feedback control are increasingly being used in medical equipment, reflecting a trend seen throughout industries [14]. Smart and self-modifying mechanisms and systems, along with improved automation and industrial manufacturing, knowledge exchange, and data management, is gaining popularity among corporations and institutions [15]. Cybersecurity is an unavoidable issue that must be addressed as the IoT evolves [16]. It's important to keep this problem under control, or otherwise hackers would use the flaws and weaknesses of devices and objects to inject false data or crash systems all over the world connected by the IoT [17].

The government, military, education, finance, healthcare, manufacturing, transportation, and more may all benefit from it [18]. Applications for cyber security rely heavily on IoT in which one of the most complicated and rapidly developing fields of computer science; data transfer is a stumbling block for IoT-style applications [19]. The IoT bridges the gap between the digital and real worlds through it, the virtual and the real can communicate with one another. Patients' records are compiled from a variety of sources in IoT healthcare apps [20]. IoT healthcare applications collect data about patients from a variety of sources, compile it into an Electronic Health Record (EHR) and then store or make it available via the internet [21]. The term "Electronic Health Record" (EHR) refers to a standardized database that contains a patient's health records in an organized fashion [22]. Most importantly, it is a computerized version for records that can be shared across other hospitals [23].

This research has the following primary contributions:

- The Intelligent Cybersecurity Standard for the Healthcare Sector [ICS-HS] is a proposed new framework in light of the increasing frequency and sophistication of cyberattacks.
- IoT advancement is impossible without first guaranteeing the security of its numerous components hence this problem can be overcome by means of ICT
- This research assessed the risks to smart health devices' security and recommends ways to lessen such dangers.

The Introduction to Cybersecurity Standard is introduced in Section 1. Next section 2 discusses the background research of different authors proposal. Design and implementation of the proposed enhanced Cybersecurity Standard are described in Section 3. Section 4 illustrates software performance testing and analysis. This paper concludes and outlines directions for further studies in Section 5.

2. Literature View:

Several researchers' works are discussed in this section. In this research, the available models and the various approaches to data analysis are discussed.

Lu, Y et al. [24] examines the safety of internet-connected devices [S-ICD]. Protecting and integrating disparate ICT and smart gadgets are the paradigm's key tenets. Our findings are relevant to everyone concerned with the safety of IoT devices and discuss issues such as the current state of the art in IoT cybersecurity research, the architecture and taxonomy of IoT security, the most effective countermeasures and strategies, the most important industry applications, and the most pressing research challenges. The IoT has the potential to improve many aspects of modern life, including availability, scalability, security, privacy, and interoperability.

Kuzlu, M et al. [25] developed and present a follow up of the relevant literature in the disciplines IoT and AI and attacks using and against AI [IoT-AI] by compiling data from a number of different surveys and research on these subjects. Yet, cybercriminals have learned to take advantage of AI and even employ antagonistic AI in their attacks. The development of complicated algorithms to safeguard networks and systems, especially IoT devices, is at the forefront of cybersecurity thanks to Artificial Intelligence (AI).

Thomasian, N. M et al. [26] exhibited the primary aim of this research is to evaluate the effectiveness of current policy [E-IoMT] approaches for protecting IoMT technologies. Due to advancements in detecting and acting technology, a new generation of medical gadgets has emerged thanks to the IoT. Cyber hazards in this hyper connected environment must be preemptively mitigated to ensure sustained patient safety. The medical cybersecurity literature was assembled for a qualitative research, including legislation, political sciences, industry guidelines, cyber breach assessments, and participant scientific journal research.

Sreedevi, A. G et al. [27] introduced Cognitive Computing (CC), a branch of artificial intelligence, is a powerful tool for overcoming these obstacles because of its role as a key driver in the automation of tasks requiring extensive knowledge. One of the first things researchers need to do to make progress in CC is to become familiar with the most recent research and the state of the art in the field. As such, this paper gives a thorough overview of previous studies in the CC domain, including its issues, solutions, and potential future directions for research. In particular, the healthcare, cybersecurity, big data, and IoT application domains where CC-based techniques have been used to solve real-world challenges have been explored in depth, and the open research issues have been discussed.

Boudko, S et al. [28] produced studies adaptive security for key healthcare infrastructures to prevent and deal with evolving threats. The Adaptive Cybersecurity Framework [ACF] is suggestion for a system that can change in real time to counteract cyberattacks. Next use evolutionary game theory to model and assess the framework, and conclude by outlining next steps for development. The IoT poses new security challenges due to its ability to connect people, processes, devices, and data, and it has the potential to greatly enhance the susceptibility of healthcare services.

In spite of the current existing models S-ICD, IoT-AI, E-IoMT, CC, and ACF there are some drawbacks in security and other issues. Hence this paper framework named Cyber security using the ICS-HS for healthcare sector has been proposed after extensive research. This proposed model design, which is supported by verifiable mathematical formulations and diagrams which outperforms the state-of-the-art techniques of the existing methodologies.

3. Intelligent Cybersecurity Standard for the Healthcare Sector:

Modern technology is more advanced and effective at assisting humans in a wide range of tasks, both at home and work. With the advent of Artificial Intelligence [AI] came the widespread adoption of smart gadgets across industries on the premise that computers could one day outperform humans in decision-making. From the findings of this research, it is recommended that the healthcare sector adopt the Intelligent Cybersecurity Standard (ICS). Cybersecurity is spread in its entirety, from end to end, which has allowed for contact and interaction between potentially malicious parties. When it comes to sharing patient information, healthcare providers like hospitals and clinics can benefit greatly from an in-depth standard approach that incorporates the IoT, allowing for the secure collection, storage, and distribution of medical data from healthcare and integrated devices.

$$\mathrm{R}(\mathrm{p},\ \emptyset * \mathrm{q} + (1 - \emptyset) * \mathrm{p}) = \mathrm{R}(\mathrm{q},\ \emptyset * \mathrm{q} + (1 - \emptyset) * \mathrm{p}) \quad (1)$$

Dynamic populations of players with a spectrum of strategies can be modeled using evolutionary game theory in the above equation (1). In this it indicates that p is the strategy for game R where Q indicates the opponent in game

playing and ∅ mentions the indicator. Here, populations change depending on how well different strategies are doing overall.

A strategy p is any strategy $P \neq Q$ a critical mass of mutants has been reached.

$$\frac{\partial p\,(t)}{\partial t} = \left(R(p_i) - R_A(p) \right) * p_i(t) \qquad (2)$$

The above equation (2) captures a central idea of replicator dynamics. This formula has three variables: p_i, $R(p_i)$, and R_A (x), where p_i is population strategy I percentage p = (p1;:::pn) and $R(pi)$ is the expected utility of strategy i. $\frac{\partial p\,(t)}{\partial t}$ is the probability of strategy when multiple members of a population engage in a given activity, they can learn from one another's actions by comparing their strategies to the mean population outcome. They can use the replicator dynamic equations to rethink their tactics. Therefore, the equation is the controlling factor in how the strategies evolve over time.

With the development of IP protocol and sensor networks, as well as the proliferation of internet and wireless communication, smart devices, and objects, IoT cybersecurity has expanded to include a wider variety of network-based items. The IoT is a global infrastructure of diverse smart devices that integrate sensing, communication, networking, and computing capabilities. The IoT is a global network of interconnected devices that may collect and process data as well as perform other useful tasks such as sensing, communication, networking, and computation. IoT incorporates a wide variety of different technologies and gadgets that all have an impact on cybersecurity, including barcodes, smartphones, social networks, and cloud computing.

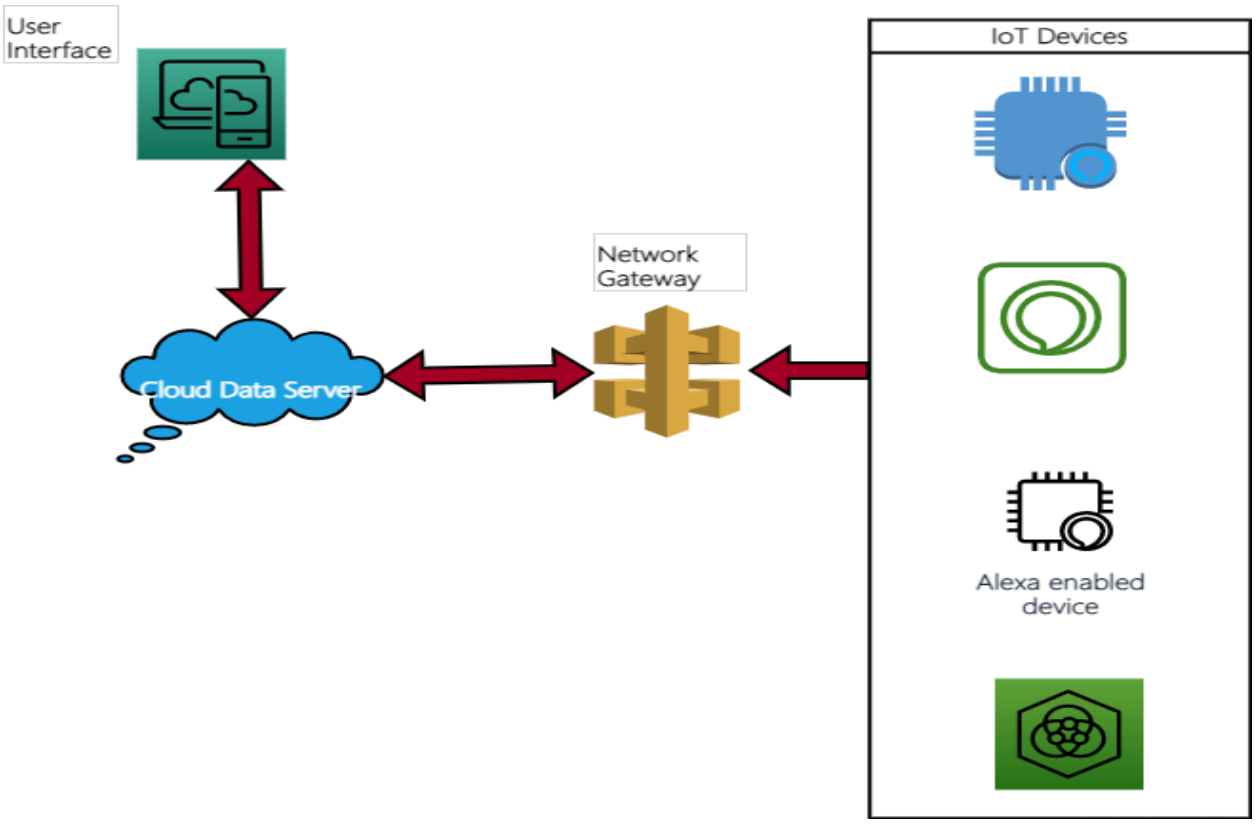

Figure 1: General structure of the IoT

An overarching diagram of an IoT system is shown in Figure 1; most of the attacks discussed in this paper focus on the gateway node and/or cloud data service connectivity, as these are often the weakest areas in IoT security. As a result of inadequate protections implemented in many IoT gadgets, cybercriminals have discovered a wide variety of entry points through which to launch attacks. Typical attack vectors in an IoT system include the IoT device (including its hardware and software), the network to which the gadget connects, and the application with which the device interacts. As a first step in any cyberattack against an IoT device, attackers will often conduct research on the device to find its weak points.

$$Inf_{a,b} = E_s(C, S)$$

$$EC_s(C, S) = DC_s\left(D_a(N, N_a, N_b)\right) \quad (3)$$

Symmetric encryption S is shown here for the information $a\ and\ b$ be the two points taken for consideration which must be protected from the Information detection Inf (a, b), and EC is shown for the encrypted data. Information can be kept in the cloud, which is a data storage facility accessible over the Internet C. To decrypt encrypted data $(\mathrm{N}, \mathrm{N\ a}, \mathrm{N\ b})$ using a key-value pair Private keys for the asymmetrical decryption DC_s scheme are held separately by the client and the provider D_aN.

This is typically accomplished by acquiring a commercially available copy of the IoT gadget that is the target. They then use their newly-gained knowledge to devise a test attack on the device to see what kind of data can be extracted from it and where potential vulnerabilities lie.

With the help of IoT, disparate smart devices may be brought together to form a secure network. Cybersecurity in the IoT is a framework for the systematic enhancement of all IoT-related modifications and a means of guaranteeing their overall security. Despite (or maybe even because of) the internet's many advantages, the worldwide IoT network is vulnerable to security breaches and malicious activity in the absence of robust cybersecurity architecture and services. Our analysis finds cybersecurity countermeasures and IoT strategies used in many businesses and it shows the difficulties and potential rewards for future researchers in this area.

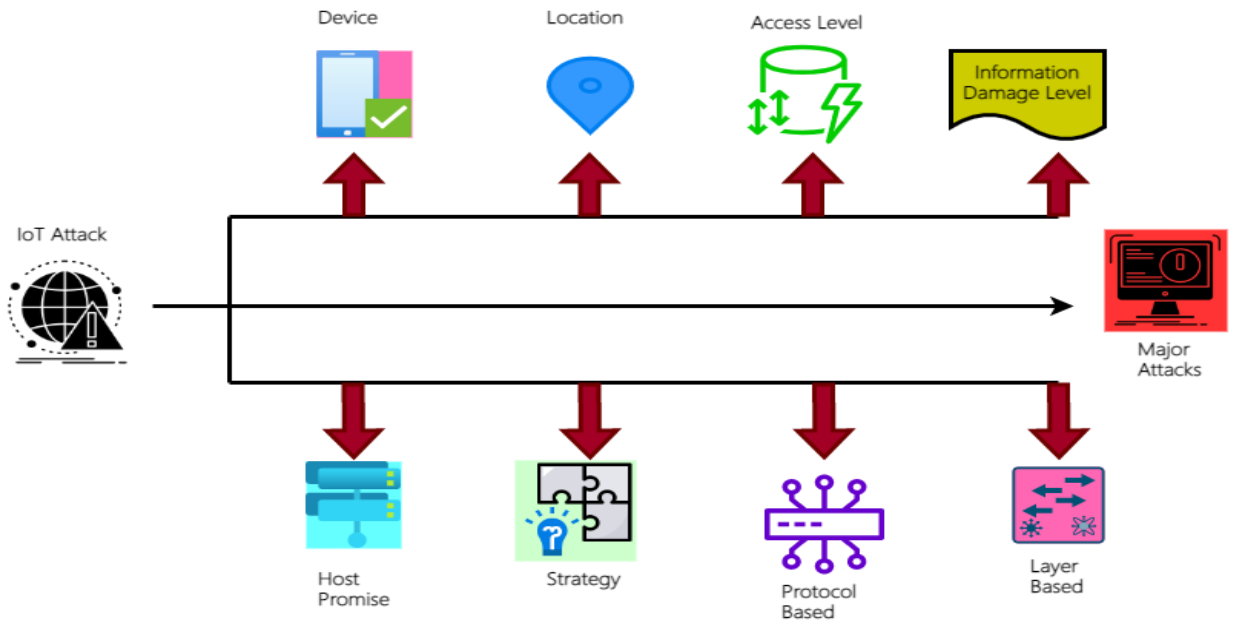

Figure 2. IoT Cybersecurity Threats

Because of the large variety of smart devices, protocols, applications, and services, there is a sizable pool of potential victims for these kinds of assaults which is shown in figure 2 as above. Our classification system for attacks includes eight distinct groups ,when it comes to devices, there are two types of attacks: sophisticated and amateurish. There are two types of location-based attacks: internal and external. Attacks that target a specific access level can be either active or passive. Interruptions, eavesdropping, modifications, fabrications, replays, and man-in-the-middle assaults all cause information damage. To launch a host-based attack, one must utilize a user, hardware, or software. There are two types of attacks based on strategy, one physical and one logical. Disruption and deviance are the hallmarks of protocol-based attacks. Layer-based attacks include those that target a user's perception, network, middleware, or applications. When an assault is launched on an IoT system, the quality of the equipment used to access it determines whether or not it is considered high-end.

There are two types of risks to the IoT network: There are two types of network security threats: internal, which come from within the network, and external, which come from outside it. The goal of an internal assault on an IoT network is to execute malicious code on devices under the attacker's control. Internal attacks can come from four different directions: those from those in impacted roles, those from those in inadvertent roles, those who attack on the basis of emotion, and those who attack on the basis of technical knowledge. IoT smart devices are targeted by an attacker who attempts to get unauthorized remote access to them from outside the network.

$$Rep = \partial_{AB} + L_t - ((1\%\ \partial_{AB}) * \partial) \times L_t \quad (4)$$

High levels of trust between parties are necessary for smooth exchanges of IoT data. Thus, the healthcare industry can evaluate the reliability of potential partners by employing trustworthiness assessment strategies. The Rep indicates report which places a premium on the veracity of potential medical care. If doctor have objective confidence in a person's abilities ∂_{AB} , the trustworthiness denoted by L_t of that person is the tanding factor (∂). In the first place, the equation (4)-mentioned it consults allow for a trust assessment service to be applied to patient records. If all the relevant data can be hacked into, then trust assessments can take place.

$$D_m(sn) = [D_m(hi) \times A_m + hc_m fr_m(t)] - 1 \quad (5)$$

Sensors sn are deployed in predetermined locations to collect data D_m and healthcare sensors hc_m. To aid with this process, sensors have been strategically placed throughout the area A_m. A regular schedule of bed rest is required due to chronic health issues (hi). The discomfort, stress $fr_m(t)$, and restlessness that bed rest can bring to patients are defined by equations (5) and (6).

$$D_m = \frac{\max\,[sn + D_m(t)]}{2} \quad (6)$$

The patient and their bed are both equipped with sensors to track their movements. Healthcare sensors hc_m and medical equipment frequently suffer from resource limitations, making them vulnerable to malicious attacks. A_m like eavesdropping, interference, and malware and worm threats.

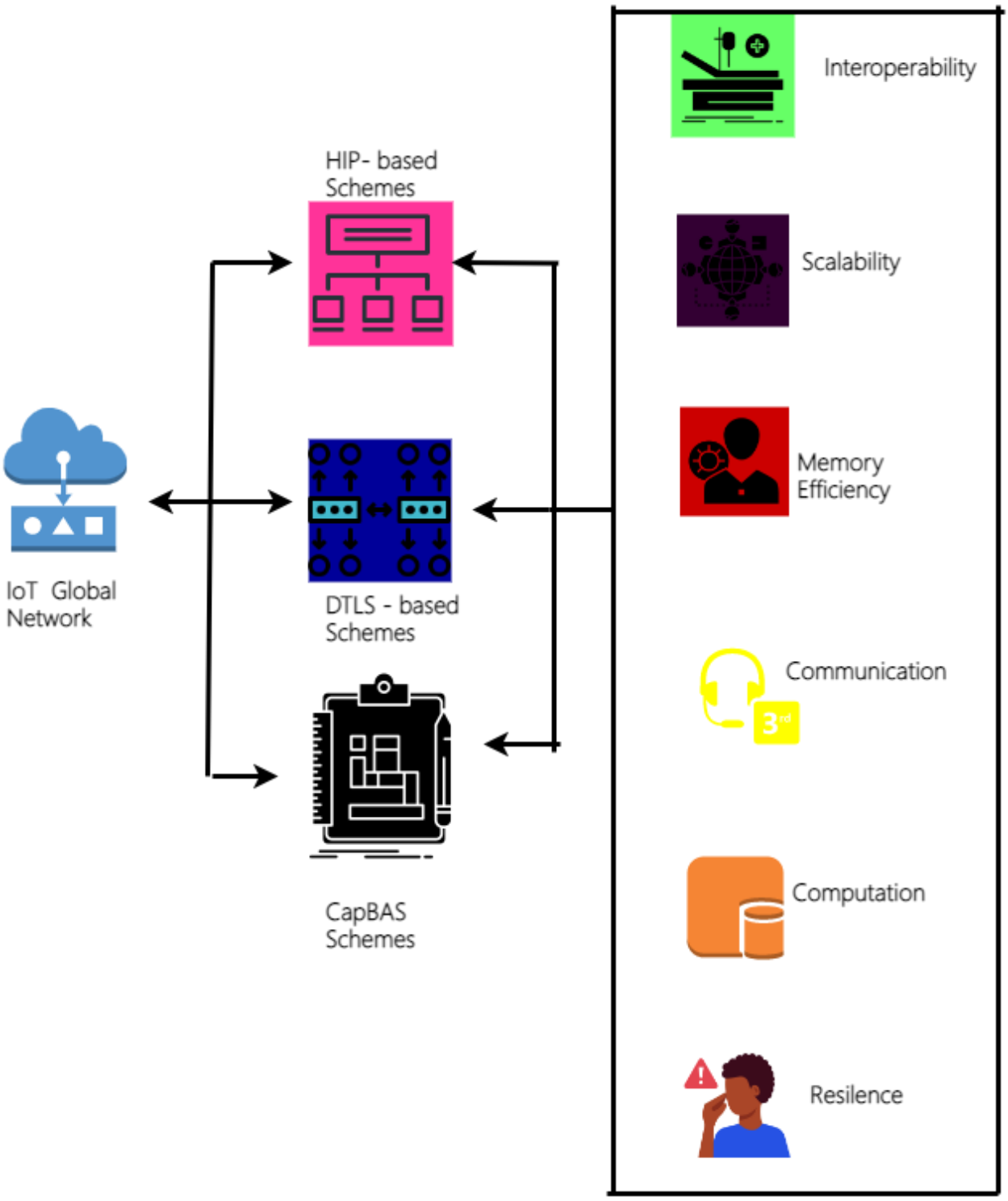

Figure 3. IoT Security Strategies Assessment Framework

In figure 3 the plans are described, as are their benefits and drawbacks. This is a sample evaluation chart. Here present a broad overview of IoT security, splitting it up into three categories: those based on the Host Identity Protocol (HIP), those based on Datagram Transport Layer Security (DTLS), and those based on Capability-based Access Control (CapBAC).

HIP scheme:

These approaches are applied to IoT device authentication based on device mobility security properties such interoperability, the difficulties of scalability, memory usage, processing time, and failure, and durability. Slim fit's advantages of robustness, memory and connectivity make it a possible choice for the IoT, the protocol's lack of scalability and compatibility makes it less attractive. Due to its computational complexity, HIP-high DEX may be well-suited for the IoT since it can achieve very high levels of interoperability, resilience, scalability, communication complexity, and memory.

DTLS scheme:

With the introduction of a new standard for the IoT, DTLS-based (Datagram Transport Layer Security) techniques are developed to ensure the safety of the IoT infrastructure. Interoperability, resilience, scalability, communication, memory, and computation are all features that must be met by DTLS-based schemes in the same way as they must be met by HIP-based schemes. In a home network, a Delegation Server (DS) acts as a trusted third party to verify certificates. Improved interoperability, robustness, and scalability are all benefits of certificate-based DTLS systems, these systems have significant limitations in other areas, including compute, communication, and memory. Delegation-based DTLS methods, on the other hand, benefit from improved read/write performance, computational efficiency, and memory efficiency. Nevertheless, delegation-based systems

CapBAC scheme:

In the IoT Capability-based Access Control is the technique by which authorized users are granted access (CapBAC). Access control system CapBAC safeguards credentials with a cryptographic token. Two types of CapBAC schemes exist: those that are centralized, in which the accessibility control logics are investigated in a centralized Cloud entity, and those that are distributed, in which the access control logics are embedded in IoT smart devices. Interoperability, computational complexity, and memory efficiency are all satisfied by a centralized strategy. Yet, there is a need to amplify the data transfer between smart gadgets and the outside world. In contrast, a distributed method can scale well isn't as interoperable or memory-efficient.

$$Ind_{val} = (lpv(h), T1 - T2) = PY(p1 - pn) * W \quad (7)$$

The equation (7) states that patients with a lower patient value (lpv) and $T1$, $T2$ be the temperature of patients at two levels respectively are in worse health than those with a higher health index value (Ind_{val}), where p is the patient's subjective assessment of his or her own health h and weight W (7). Medical personnel need to be alerted whenever there is a potential risk to a patient's health hence that they can take the necessary measures. Conditional probability (PY) can be calculated from the index values $(p1 - pn)$ using the average weight (W) method.

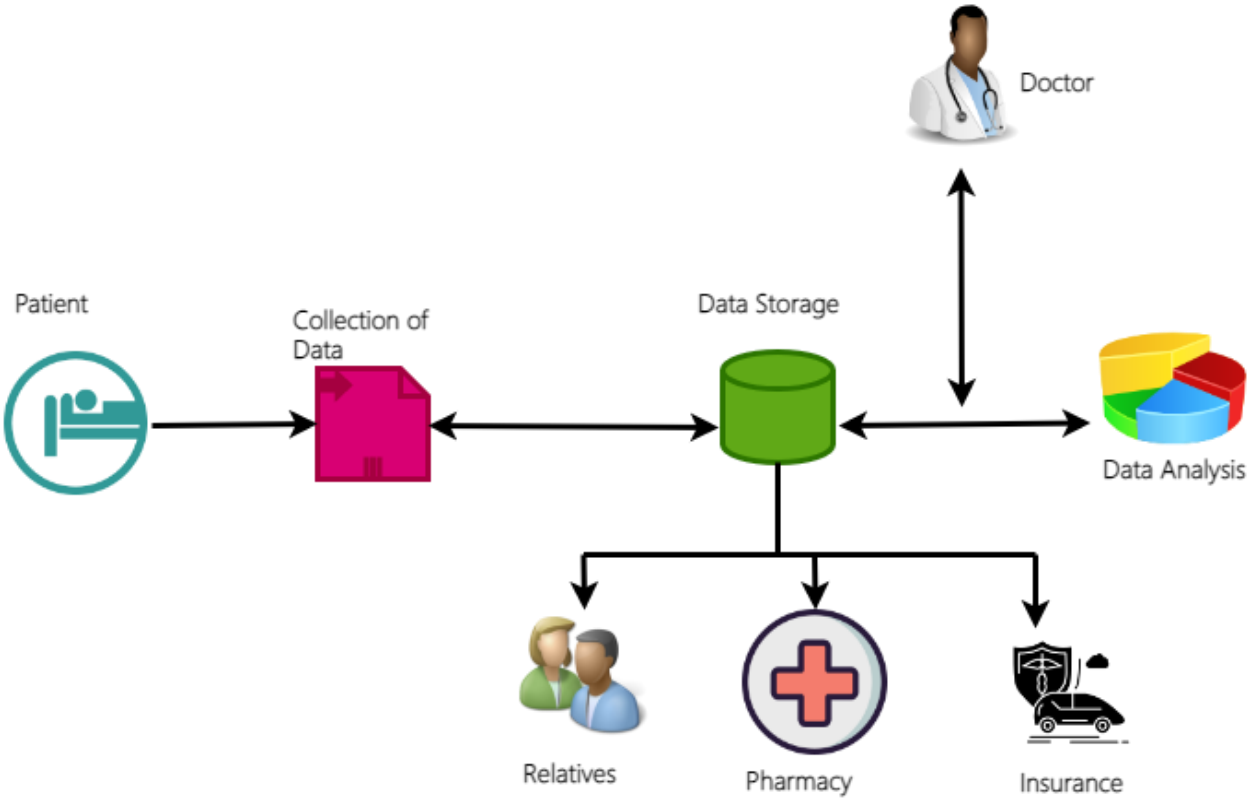

Figure 4. Integrating Intelligent Healthcare Components

IoT-based smart healthcare networks typically include three basic components for Information gathering, data preparation, data processing and data analysis. Figure 4 provides an overview of the components of smart healthcare.

Acquisition and Pre-Processing of Data:

Data is gathered from the patient via sensors, detectors, or monitors. In the instance that the patient is in an outlying area, sensors will be included in the wearable devices. If the gadget is not accessible, the patient may need to be physically present at areas with available devices for the data to be uploaded to the network. At the patient end, data collection transceivers may either immediately transmit the data or analyze the data locally before sending the processed information to a data storage center. To make matters more manageable, the information will be transformed into a transmission-friendly format. Information security requires that data be encrypted before to transmission.

Processing and storing of data:

The patient's information obtained will be sent to the data storage facility. It's likely to be some kind of cloud-based storage service. The information will then be sent to the person or group that has a legitimate need for it after being processed. Based on who is using the information, it will be presented in a different format. There's no guarantee that the information supplied to a doctor is the same information sent to loved ones. The data storage media will take the doctor's comments into account and relay the relevant information to the right persons. Data can be sent to the patient, the hospital, family members, insurance companies, or anybody else specified in the network that needs to know.

Analyzing of Data:

The doctor or research team treating the patient will analyze the collected data to determine the efficacy of their care. There are a variety of research applications for this information as well as behavioral analysis. The patient's future health status can be predicted with this information.

$$S_i(x) = D(Rms) - \sum \sqrt{(Rms)^{1/2}}.t_i(Rms) \quad (8)$$

With the help of S sensors, (x) can analyze data from a large number of devices in a distributed setting using equation (8). This system provides a wide variety of options and capabilities that can be used to improve the computing framework at the edge networks. Hence to aid people in their daily lives, this cutting-edge technology uses W real-time discrepancy detection. IoT-based (Rms)have been proven to provide patients with accurate data D and timely t in remote monitoring systems.

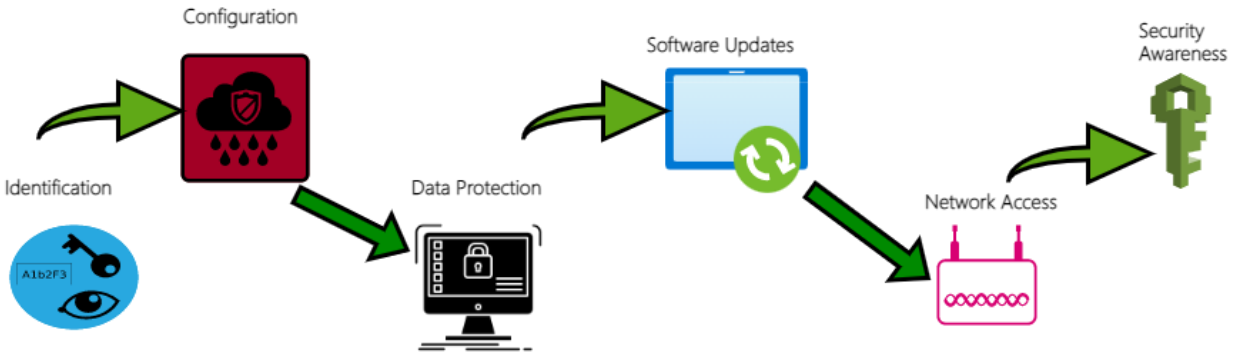

Figure 5. Cybersecurity Fundamental Principles for IoT Devices

Cybersecurity fundamental principles for IoT devices are in figure 5 as shown above. In this file, one connect hazards in the IoT threat landscape to appropriate security advice documents for all industries, with healthcare receiving the highest score for the availability of key cybersecurity standards in network and physical security. Exploration priorities include using block chain for cryptography, dealing with incidents that can't be patched, managing network connections on the fly, and automating security. Principles such as identifying devices, allowing authorized configuration, protecting data, limiting access, updating software, and detecting devices are at the heart of this philosophy. The federal government's authority over the IoT will be bolstered by future directions for cyber oversight as a whole.

$$P_q = \frac{\delta_r}{m}[b_m \mu(P * m + \delta\mu - P_{dr})]/2 \qquad (9)$$

According to (9) P is a probability of q events. The random variable δ_r with an exponential average distribution $\delta\mu$, and the care latencies m are independent and identically distributed. Providing all parts of the system with first-come first-served access to incoming health data denoted by b_m is one way to encourage this. The IoT has the distinct capacity to expand fog resources P_{dr} into the public IoT data center with μ be the probability density function.

Our proposed system, ICS-HS, combines a conventional in-depth approach with IoT and integrated devices to collect, store, and distribute medical data in a secure and distributed manner; this makes it a good option for organizations in the healthcare sector, such as nursing homes, hospitals, and the healthcare business, which often communicate this kind of information.

4. Results and discussion:

Here discuss the simulations used to test the effectiveness of the proposed ICS-HS. In this simulation, there are 70 sensor nodes and 8 user devices. The system includes the previously recommended 10-second response interval. Measures of performance include precision, security rate, security performance, success rate, and latency rate compared to traditional methods and response time. The reliability of the proposed method will be examined, and it will be compared to both contemporary and historical alternatives.

4.1 Security performance analysis:

Table (1): Security analysis

Number of Sensors	S-ICD	IoT-AI	E-IoMT	CC	ICS-HS
10	**52.3**	**65.1**	**79.1**	**89.6**	**90.2**
20	**85.9**	**75.4**	**82.8**	**84.5**	**91.1**
30	**55.5**	**65.2**	**84.6**	**92.9**	**92.5**
40	**52.3**	**73.5**	**79.3**	**87.1**	**93.4**
50	**52.6**	**64.0**	**75.1**	**82.6**	**95.5**
60	**54.1**	**75.3**	**83.0**	**95.3**	**97.9**
70	**57.9**	**68.6**	**77.5**	**89.5**	**98.8**

The suggested framework's user node security rate and monitoring intervals for IoT healthcare cybersecurity are shown in table (1) above. The model's parameters for mapping are controlled by nodes, which receive healthcare data. Mapping establishes what the user can and cannot do with their data, and the two categories—secure and insecure—are defined. By comparing patients' past data with the predicted model, one can get an idea of how much it will cost to track down specific events. Regular transfers of the provision's outcome are made, and that outcome is grounded in a high level of precision. The proposed model improves the safety of many IoT sensor networks. Based on the suggested architecture, healthcare data may be gathered and integrated to create an IoT system for authentication and cybersecurity. When a patient reports an emergency, the team immediately responds.

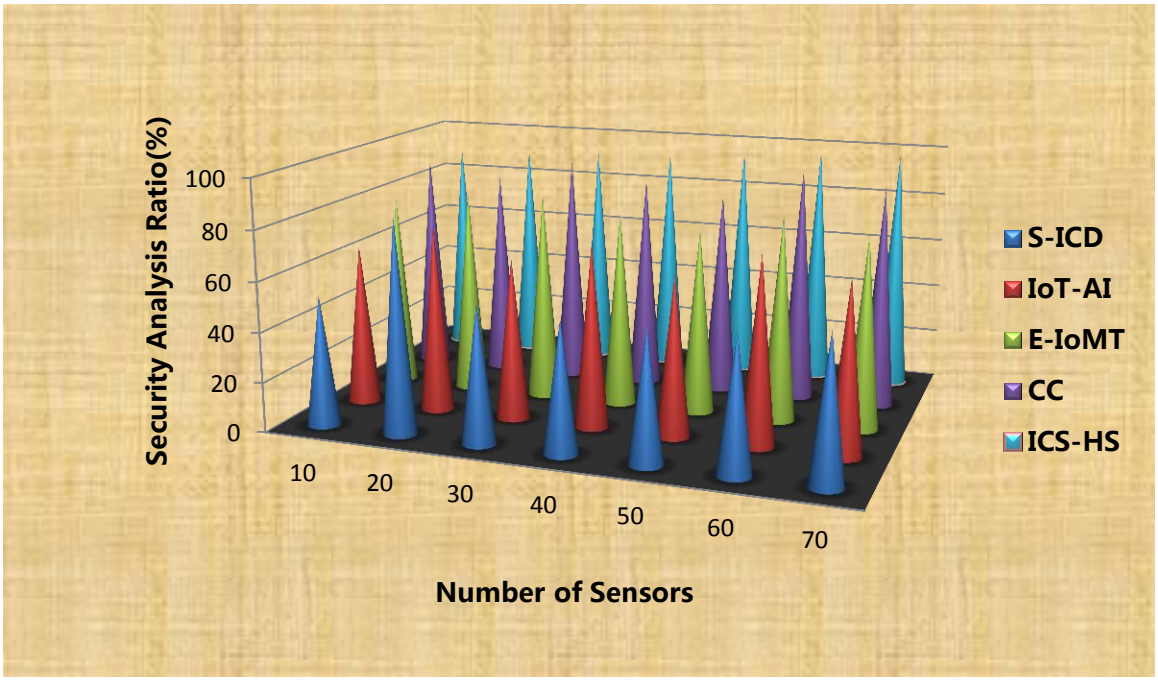

Figure 6- Security analysis

Figure (6) demonstrates how the user node operation rates and monitoring intervals are decreased and optimized in comparison to conventional IoT healthcare data security methodologies. One benefit of keeping medical records is that they help hospitals run more smoothly. Through the use of biometric indicators and the user's

preferences from the formula, they can gain access to their medical records. It is necessary to repeatedly use multiple IoT sensors to investigate a neighboring state, and the results must be recorded. Patient-specific predictions are made using information from the user nodes. Accurately monitoring the patient's activities allows for efficient use of available resources.

4.2 Examining the Rate of Latency:

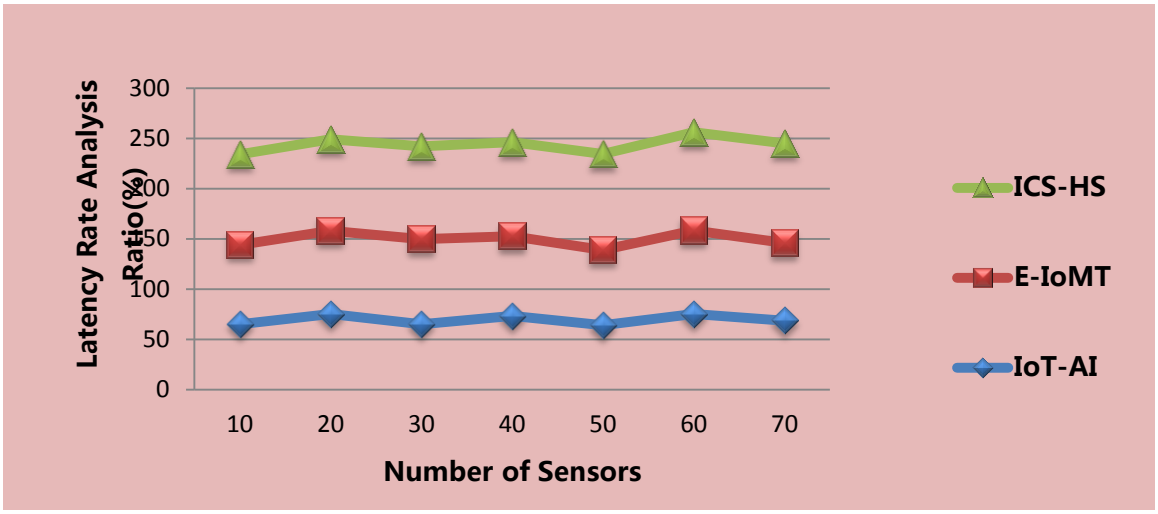

Figure 7- Variations in Latency Rate

Figure (7) shows a latency comparison between different methods and physical monitoring equipment, making it clear that the ICS-HS method is the most consistent and reliable. When put next to the norm, IoT-based external sensor-based health monitoring systems perform better when it comes to the estimated number of iterations using equations. Biometric and medical data can be either continuous or discrete, and both types of data create a reaction space for the points. The purpose of this research is to present the ICS-HS paradigm for securing IoT sensor networks in healthcare environments which is based on the principles of public health care data protection and privacy. This model is based on the IoT and aims to boost healthcare safety.

4.3 Prediction analysis:

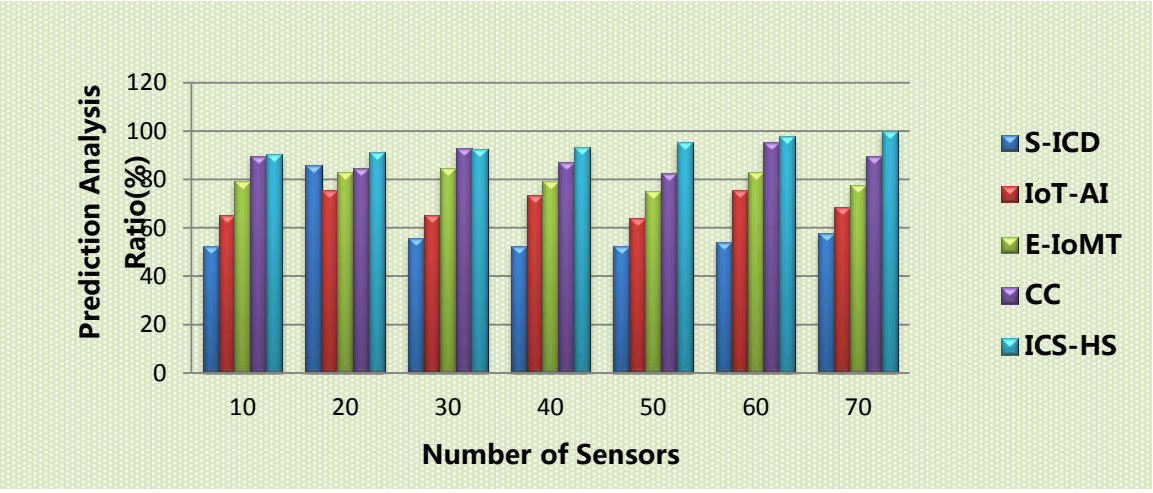

Figure 8- Ratio of Sensor Prediction Time

Figure 8 illustrates the many ways in which better information access can lead to better health outcomes, such as earlier diagnosis and more effective treatment, as well as deeper understanding of the underlying causes of disease. Predictive medical analytics can predict ward decline by identifying high-risk patients at home and discouraging readmission. As a result of having much data at their disposal, medical professionals and institutions are now better able to diagnose conditions and provide timely, effective treatment. Researchers can gain a deeper understanding of disease mechanisms, improving their ability to foresee health problems. Data analysis, predictive modeling, and deep learning are just some of the methods used in predictive analytics.

4.4 Effectiveness Analysis:

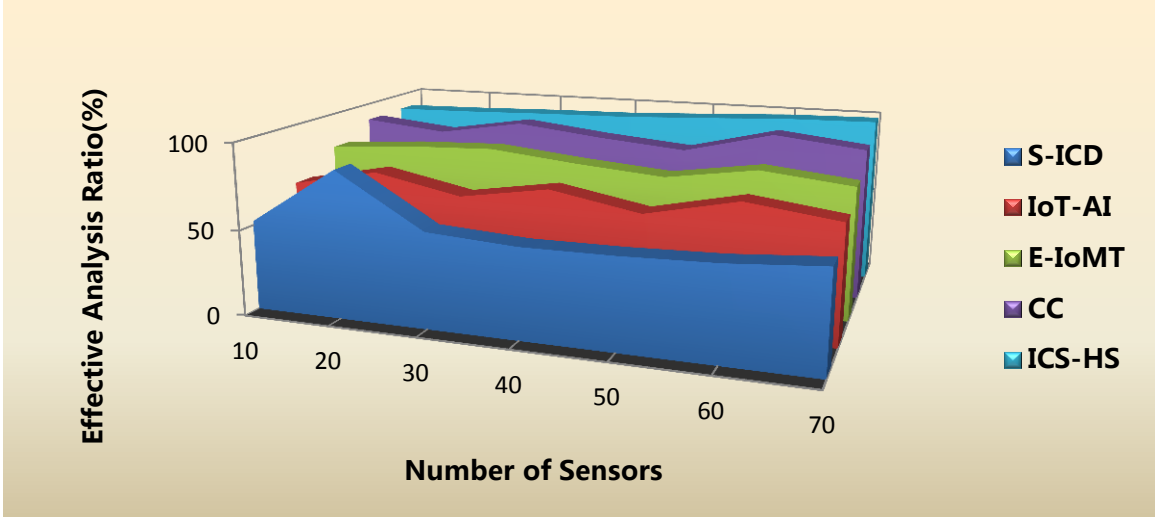

Figure 9 - Effectiveness Analysis Ratio

Figure 9 shows that the ICS-HS method performs better than the conventional method in terms of standardization and efficiency when it comes to physical health monitoring systems. Compared to more traditional monitoring methods when it comes to health monitoring, IoT systems based on real sensors have been shown to be superior over an estimated number of repetitions using equations.

4.5 Performance Analysis:

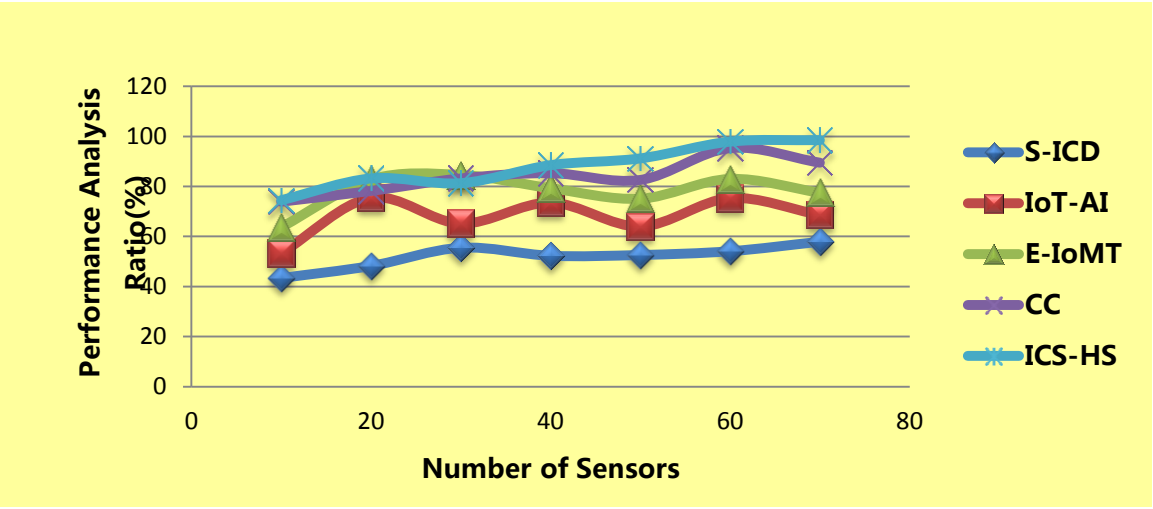

Figure 10 – Performance Analysis Ratio

A graph depicting a performance analysis is plotted, showing how various existing proposed methods fare when applied to a wide range of data sets as shown in figure 10. The equations show that ICS-HS performs 98.8% better than other methods.

When comparing the efficiency of S-ICD, IoT-AI, E-IoMT, CC, the proposed ICS-HS, the latter is found to be superior in terms of security, latency, predicting behavior, analysis of execution time, and performance in a smart environment. When comparing the new model to the traditional approaches to protecting healthcare data in the IoT, its many advantages become clear.

5. Conclusion:

Key elements of a dynamic cyber security framework for healthcare IoT infrastructure protection are outlined in this paper. The optimal defensive reaction against dynamic and adaptive attacks has been simulated here. Multiple attacks have been developed against IoT systems, and more are likely to be found as the popularity of IoT rises. Protecting systems from these kinds of attacks is essential. Hence to protect these systems in an intelligent and real-time manner from the increasing experts are increasingly relying on AI to counteract the growing number and speed of attacks. Adversaries develop countermeasures and even employ artificial intelligence in their attacks. This paper takes a look at the typical approaches taken by attackers in an effort to disrupt or compromise IoT, and gives a brief summary of how these assaults function. The benefits of "smart healthcare" are numerous, including expedited diagnosis, better decisions, and preventative care. Cybersecurity plays a pivotal role in these kinds of networks. This paper applies the Intelligent Cybersecurity Standard for the Healthcare Sector which improves the speed and accuracy of health monitoring, to facilitate prompt, effective care. This paper examines the components of Smart HealthCare networks and the risks to their cyber security. Preventative steps to strengthen the safety of Smart Healthcare networks are discussed. The offered preventative measures can serve as best practice guidelines when creating a safe Smart Healthcare setting. In the future, one plan to model the evolutionary dynamics of adaptive attacks and defenses using machine learning and evolutionary game theory, as well as to develop appropriate quantitative metrics and conduct game simulations.

References:

1. Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. *Applied Sciences*, *12*(3), 1598.
2. Williams, P. A., & McCauley, V. (2016, December). Always connected: The security challenges of the healthcare Internet of Things. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)* (pp. 30-35). IEEE.
3. Jackson Jr, G. W., & Rahman, S. (2019). Exploring challenges and opportunities in cybersecurity risk and threat communications related to the medical Internet of Things (MIoT). *arXiv preprint arXiv:1908.00666*.
4. Nasiri, S., Sadoughi, F., Tadayon, M. H., & Dehnad, A. (2019). Security requirements of internet of things-based healthcare system: a survey study. *Acta Informatica Medica*, *27*(4), 253.
5. Salam, A., & Salam, A. (2020). Internet of things for sustainability: perspectives in privacy, cybersecurity, and future trends. *Internet of things for sustainable community development: wireless communications, sensing, and systems*, 299-327.
6. Kelly, J. T., Campbell, K. L., Gong, E., & Scuffham, P. (2020). The Internet of Things: Impact and implications for health care delivery. *Journal of medical Internet research*, *22*(11), e20135.
7. Ferrag, M. A., Friha, O., Maglaras, L., Janicke, H., & Shu, L. (2021). Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis. *IEEE Access*, *9*, 138509-138542.
8. Billingsley, L., & McKee, S. A. (2016). Cybersecurity in the clinical setting: Nurses' role in the expanding "internet of things". *The Journal of Continuing Education in Nursing*, *47*(8), 347-349.

9. Monteith, S., Glenn, T., Geddes, J., Severus, E., Whybrow, P. C., & Bauer, M. (2021). Internet of things issues related to psychiatry. *International Journal of Bipolar Disorders*, *9*(1), 1-9.
10. Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65-88.
11. Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), 4580.
12. Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer law & security review*, *32*(5), 715-728.
13. Mcgowan, A., Sittig, S., & Andel, T. (2021). Medical internet of things: a survey of the current threat and vulnerability landscape.
14. Aldaej, A. (2019). Enhancing cyber security in modern internet of things (iot) using intrusion prevention algorithm for iot (ipai). *IEEE Access*.
15. Zhan, K. (2021). Sports and health big data system based on 5G network and Internet of Things system. *Microprocessors and Microsystems*, *80*, 103363.
16. Sharma, A., Kaur, S., & Singh, M. (2021). A comprehensive review on blockchain and Internet of Things in healthcare. *Transactions on Emerging Telecommunications Technologies*, *32*(10), e4333.
17. Hogan, M., Piccarreta, B., & Interagency International Cybersecurity Standardization Working Group. (2018). *Interagency report on status of international cybersecurity standardization for the Internet of Things (IoT)* (No. NIST Internal or Interagency Report (NISTIR) 8200 (Draft)). National Institute of Standards and Technology.
18. Terry, N. P. (2016). Will the internet of things transform healthcare. *Vand. J. Ent. & Tech. L.*, *19*, 327.
19. Aliero, M. S., Qureshi, K. N., Pasha, M. F., & Jeon, G. (2021). Smart Home Energy Management Systems in Internet of Things networks for green cities demands and services. *Environmental Technology & Innovation*, *22*, 101443.
20. Tschider, C. A. (2018). Regulating the internet of things: discrimination, privacy, and cybersecurity in the artificial intelligence age. *Denv. L. Rev.*, *96*, 87.
21. Zhao, S., Li, S., Qi, L., & Da Xu, L. (2020). Computational intelligence enabled cybersecurity for the internet of things. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *4*(5), 666-674.
22. Boukerche, A., & Coutinho, R. W. (2020). Design guidelines for machine learning-based cybersecurity in internet of things. *IEEE Network*, *35*(1), 393-399.
23. Bakar, N. A. A., Ramli, W. M. W., & Hassan, N. H. (2019). The internet of things in healthcare: an overview, challenges and model plan for security risks management process. *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, *15*(1), 414-420.
24. Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103-2115.
25. Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of things*, *1*, 1-14.
26. Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the internet of medical things. *Health Policy and Technology*, *10*(3), 100549.
27. Sreedevi, A. G., Harshitha, T. N., Sugumaran, V., & Shankar, P. (2022). Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review. *Information Processing & Management*, *59*(2), 102888.
28. Boudko, S., & Abie, H. (2019, May). Adaptive cybersecurity framework for healthcare internet of things. In *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)* (pp. 1-6). IEEE.