IoT Security

Sandeep Kumar Mangalapally
Computer Science and Engineering
Chandigarh University
Mohali, India
21BCS9608@cuchd.in

Harshitha Thadishetty
Computer Science and Engineering
Chandigarh University
Mohali, India
21BCS5848@cuchd.in

Nageswara Reddy Kasu
Computer Science and Engineering
Chandigarh University
Mohali, India
21BCS5714@cuchd.in

Nandini Bujunuri
Computer Science and Engineering
Chandigarh University
Mohali, India
21BCS4229@cuchd.in

***Abstract*—IoT is a study area that is currently receiving a lot of interest. Numerous researchers have looked at the various aspects of this topic in recent years. In the meanwhile, this technology has features that give these gadgets privacy and security. If we don't provide the necessary security, it's possible that these devices' advantages may be misused, rendering them useless. The Internet of Things (IoT) has created a world of limitless opportunities for applications across many facets of society, but it also comes with a number of difficulties. Security and privacy are two of such issues. IoT devices are more vulnerable to attacks and security issues. Due to IoT device limitations in terms of size, power, memory, and other factors, there aren't many security solutions that work with IoT devices and applications, which is turning this world of securely linked things into the "internet of insecure things." Going beyond the conventional or standard procedures and integrating security measures into the IoT device's hardware is a viable approach to this issue. IoT networks' adoption of cutting-edge technologies, such as machine learning, Blockchain, fog, edge, and cloud computing, as well as quantum computing, have increased the number of weak spots in the network. In-depth research on IoT security threats and solutions is presented in this article. This survey also describes the obstacles that have arisen from the integration of developing technologies like machine learning and blockchain with IoT, as well as possible solutions to these problems. The four-layer IoT architecture is used as a guide in this study to pinpoint security problems and suggest remedies.**

***Index Terms*—Keywords: IOT Networks, Blockchain, Machine Learning.**

I. Introduction

IoT apps are being used by more industries, thus there will be a growth in IoT devices and applications. Wearable technology with tools to track and share a person's actions and medical data, One company that offers wearable technology is sharing a person's behaviour and health data. Patients in the healthcare sector have access to IoT apps and devices. Smart refrigerators, smart heating, smart gardening, video doorbells, personal assistants for smart lights, smart coffee makers, and smart door locks are among the "smart house" IoT goods currently on the market. Some of the "smart city" apps and IoT devices that have been developed include smart parking, smart street lights, and smart waste management.

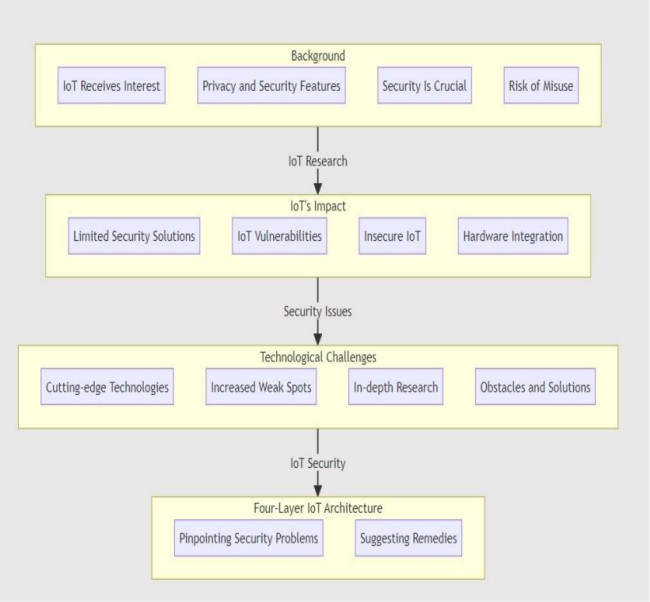

Fig. 1. Overview on IoT security with a Flowchart

IoT devices are becoming more and more commonplace today, and their use in commerce is rising. As the number of IoT devices grows, security issues become more of a concern. The firms are being increasingly breached by the attackers using the vulnerable web resources. Recurring attacks on linked devices have already been reported, and they will continue to happen if corporations do not enforce discipline in security issues. A regular buyer must be aware of the immune state of Internet of Things devices and all of its offshoots. The survey's findings indicate that the manufacturers of the devices were not entirely focused on ensuring security, which will expose customers to the possibility of intrusion or assaults. We divided all IoT devices into four different authority based on our analysis: The results show that one gadget in each group showed susceptibilities over the majority of groupings. Therefore, based on this study, we can conclude that we need

to do research on the security of device design and develop ways to minimise the risk to consumers. The current trend indicates that IoT is having a huge impact on people's lives and that it will continue to reveal fresh, creative scientific and technological advances that are built into the functionality of smart gadgets and internet-connected applications. The internet is continually absorbing revolutionary innovations like robotics apps, contactless payment systems, big data analytics, artificial intelligence, etc., making a vast amount of information accessible at any time and from any location. People use and see new smart devices every day that weren't around a few years ago, and many of these devices can communicate with one another without any problems from one side of the planet to the other. The result is that the world has, As a result, the world is increasingly dependent on the internet to enable communication between systems, people, and diverse technology.

A. Problem Definition

IoT device development in recent years resulted in a harmful era, altering our interactions with the environment and providing unmatched ease and efficiency across a variety of disciplines. However, as the IoT ecosystem grows at an impressive rate, a broad range of security concerns have surfaced and require immediate attention. The need to protect the security and integrity of IoT devices and Networks has become critically important as our dependence on linked devices grows. Risks in today's environment grow huge, exposing people, companies, and crucial infrastructure to new hazards. IoT devices usually lack the robust security protections required to prevent attacks because they frequently place a higher priority on performance and connectivity. Criminals take advantage of these loopholes and manipulate weaknesses to break into systems, steal confidential information, and even enter networks, potentially causing great disruption and harm. The IoT ecosystem's mix of devices, which covers industries like healthcare, manufacturing, transportation, and consumer electronics, adds to the problems. This diverse combination operates on several platforms, uses a variety of communication protocols, and frequently operates with limited computational capabilities. It presents a significant barrier to creating an organized and complete safety framework.

Additionally, the danger landscape's dynamic nature requires the development of an active plan that can adjust to changing attack techniques and paths. The necessity for strong security measures that not only resist current threats but also identify those on the horizon is becoming increasingly urgent as hostile actors take advantage of new loopholes and attacks become more complex.

It requires a team effort from manufacturers, developers, officials, and end users to address these complex problems. Things are made more difficult by the lack of established security procedures and a lack of consumer awareness. Neglecting security upgrades could have severe consequences, including endangered data privacy. As a result, the challenge at hand is to develop innovative and complete solutions to strengthen the safety measures of IoT devices and networks. Thus, the task at hand is to create fresh and broad solutions for improving the safety precautions of IoT devices and networks. This project includes finding and fixing issues with design, establishing safe communication protocols, and putting in place effective safety measures.

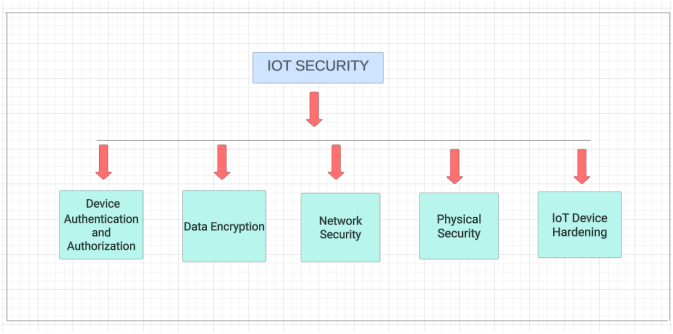

Fig. 2. Some key aspects of IOT Security

B. Problem Overview

IoT (Internet of Things) security describes the procedures and policies used to protect the confidentiality and integrity of the devices, information, and communications that make up the IoT ecosystem. The security of IoT devices is essential to preventing unauthorised access, data breaches, and potential harm because they are frequently linked to the internet and can collect, send, and process sensitive data. Following are some crucial facets of IoT security: System Security: Identifier verification and authorization to ensure that only authorised people and devices may access and control IoT devices, utilise strong authentication protocols.

Firmware updates and secure boot: To prevent unauthorised firmware alterations, ensure that devices have secure boot methods. To fix vulnerabilities, regular security updates should be made available. Device Identity Management: To prevent identity spoofing, give each device a distinct identity and administer it securely. Communication Security: Encryption: To prevent eavesdropping and data interception, all data transported between IoT devices and backend systems should be encrypted using robust cryptographic protocols. Use secure communication protocols like HTTPS, MQTT with TLS, and CoAP with DTLS to safeguard the confidentiality and integrity of your data. Network segmentation: To lessen the possible impact of a compromised device, isolate IoT devices from crucial business networks. Data Security: Data Encryption: To prevent unauthorised access, data stored on Internet of Things devices or transmitted across networks should be encrypted. Data minimization: To lower the risk of potential breaches, just collect and keep the information that is required. Secure Data Storage: Ensure that data storage systems, whether they are on the device or in the cloud, adhere to best security practises. Designing devices with physical protection features to thwart tampering and unauthorised access to device components will increase physical security and tamper resistance.

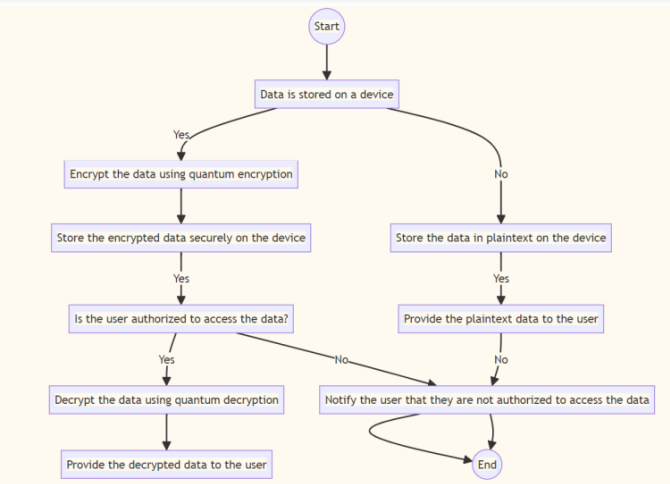

Fig. 3. Procedures for securing and accessing data stored in device

C. Hardware Specification

Neural Processing Units (NPUs): These are specialized chips designed specifically for handling AI and machine learning tasks. With the increased reliance on AI for adaptive security protocols and behavior analysis, NPUs can accelerate these tasks, making real-time threat detection and mitigation more feasible. Hardware Needed: Secure Servers and Network Equipment What do they do? Secure Servers: These are like big electronic storage rooms where companies keep and share safety information. They need to be super secure so that only trusted people can access the data. Network Equipment (like routers and firewalls): Think of these as the ”traffic controllers” of the internet. They decide which data can go in or out. For our purpose, they ensure that the safety data we share worldwide goes to the right place without being intercepted bad guys. Quantum Processors: For quantum-resistant cryptographic methods, having hardware that understands and operates based on quantum principles can be crucial. While true quantum computers are still in development, small-scale quantum processors can be instrumental in researching and implementing quantum-safe encryption techniques. Secure Element (SE) Chips: These are dedicated chips designed to handle sensitive operations securely, such as cryptographic operations and secure boot processes. SE chips can store private keys and execute cryptographic functions, isolated from potential external threats. Edge Computing Processors: With the push for edge computing in IoT, processors tailored for edge operations are becoming vital. These are energy-efficient, capable of handling local data processing tasks, and come with built-in security features to ensure data integrity at the source.

Hardware Security Modules (HSMs): These are physical devices that safeguard and manage digital keys for strong authentication. They offer a tamper-resistant environment for cryptographic operations, ensuring that even in the case of a system breach, sensitive cryptographic material remains secure.

D. Software Specification

In order to detect problems, protect data, and create safe communication paths, a variety of software tools and technologies are used to improve IoT security. To improve IoT security, the following crucial software elements are frequently used: Device Management systems: These systems provide centralized management to oversee and keep track of IoT devices, providing remote updates, patches, and modifications. Examples to consider include Google Cloud IoT Core, AWS IoT Core, and Microsoft Azure IoT Hub Encryption and authentication are provided through the TLS/SSL protocols, which provide secure means of communication between devices and servers while guaranteeing the privacy and security of all data. Public Key Infrastructure (PKI): PKI solutions use digital certificates and keys to enable strong authentication and secure communication. Structures and Tools for Safety: utilizing TLS: This no-cost, open-source library conducts out encryption operations and protocols, improving up secure IoT device relationships. Systems for detecting and preventing intrusions (IDPS): An open-source network intrusion detection system (NIDS) that might be customized to track and shield IoT networks from malicious activity is called Snort. Suricata is a network intrusion detection system (NIDS) with real-time intrusion detection, network security monitoring, and threat detection capabilities. Using security gateways and firewalls: IoT Firewalls: These firewalls offer network segregation, traffic filtering, and protection from unauthorized entry because they were specifically created for IoT networks. Security entry points These devices serve as a bridge between IoT devices and the main network, imposing security protocols and filtering out destructive data. Using firewalls and security gateways IoT The barriers Due to their creation of IoT networks, these firewalls enable network isolation, traffic filtering, and security against unauthorized intrusion. Entry points for security As a bridge between IoT devices and the main network, these devices apply security protocols and filter out damaging data. Tools for Firmware and Software Updates: Tools that make it possible for IoT devices to update securely over the air (OTA), ensuring that the devices have the most recent security patches and fixes. A personalized approach that takes into account the special characteristics, device kinds, and communication protocols of your IoT environment is crucial for applying these software components. Establishing an effective. IoT security strategy requires integrating numerous safety measures at different levels and building a strong defence against online attacks.

II. LITERATURE REVIEW

A. Existing System

IoT security, which is essential in our digitally linked society, has evolved over time. Hardware solutions such as Trusted Platform Modules (TPM) and Hardware Security Modules (HSM) have emerged as the backbone of device safety. These preserve sensitive data and guarantee secure cryptographic operations. Furthermore, the Secure Boot procedure ensures

Fig. 4. Implementation on IoT security with quantum distribution through python

that devices only boot with manufacturer-verified software, providing a fundamental layer of trust from the device's very first boot. Shifting the attention to the network, conventional techniques such as firewalls play an important role, which is reinforced by VPNs to protect distant data transfers. Authenticating devices in this large environment is no easy task. The Public Key Infrastructure (PKI) makes this easier by providing a reliable method for device identification and trust validation. However, the sheer amount and sensitivity of data produced by IoT devices need strict security measures. As a result, encryption standards that ensure data security at rest and in transit have become commonplace. Furthermore, protocols such as MQTT have been designed to meet the special communication requirements of IoT devices. With the development of cloud computing, prominent providers like AWS and Azure have launched IoT-focused platforms. These systems not only simplify device administration, but also incorporate strict security standards, such as novel Over-the-Air (OTA) update mechanisms. As we progress, AI's proficiency in behavior analysis and anomaly detection shows promise, providing a proactive layer of protection by identifying possible threats in real-time.

Hardware-based Trusted Platform Modules (TPM) The foundation of IoT device security frequently starts at the hardware level. TPMs (Trusted Platform Modules) are specialised micro controllers built specifically for hardware security. They protect the integrity and authenticity of devices by storing cryptographic keys that are essential to the device's functionality. When an IoT device boots up, the TPM verifies the software's signature to ensure that it hasn't been tampered with, providing an initial layer of security. These microcontrollers serve as the foundation for a secure boot procedure, ensuring that IoT devices are safe from the minute they are powered on.

Secure Boot Systems The software integrity of an IoT device is critical to its secure operation. Secure Boot solutions were created to ensure that an IoT device only starts up with software that has been digitally certified by a trusted organisation - often the device manufacturer. This signature is validated before the software may be executed. If the validation fails, the device will not boot, preventing malicious or unauthorised firmware from compromising the device. This offers a strong defence against malicious efforts to modify device firmware, ensuring that only legitimate and secure software runs on the device.

Network Security with Firewalls and IDS/IPS IoT devices are, by definition, linked things. As a result, they are vulnerable to network-based attacks. Advanced firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) are used to mitigate these vulnerabilities. These measures aren't just tweaks to typical network security systems; they're frequently tuned to the specifics of IoT communications. While firewalls monitor and restrict incoming and outgoing network traffic based on predefined security policies, intrusion detection and prevention systems (IDS/IPS) go a step farther. They actively monitor network traffic for unusual activity and known risks, notifying administrators and frequently implementing pre-defined preventive measures. This real-time monitoring and reaction mechanism serves as a dynamic defence layer, which is critical in the ever-changing IoT threat scenario.

Data Protection through Encryption IoT devices are, by definition, linked things. As a result, they are vulnerable to network-based attacks. Advanced firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) are used to mitigate these vulnerabilities. These measures aren't just tweaks to typical network security systems; they're frequently tuned to the specifics of IoT communications. While firewalls monitor and restrict incoming and outgoing network traffic based on predefined security policies, intrusion detection and prevention systems (IDS/IPS) go a step farther. They actively monitor network traffic for unusual activity and known risks, notifying administrators and frequently implementing pre-defined preventive measures. This real-time monitoring and reaction mechanism serves as a dynamic defence layer, which is critical in the ever-changing IoT threat scenario.

B. Proposed System

As technology advances, so will the safety of our linked gadgets. One fascinating concept is to make more use of artificial intelligence (AI). Consider AI to be a clever security guard. It can learn from previous security concerns and change itself to better safeguard our devices. With AI, gadgets can detect and correct issues before they become critical. Also, AI might aid in the organisation and upgrading of several devices at the same time, ensuring that they all have the most up-to-date safety features. Another thought comes from the field of quantum computing. While it is still in its early stages, it has the potential to improve data security. Consider a lock that changes every time someone attempts to crack it. Quantum technologies might provide this degree of security for our data. Simultaneously, there is a rising desire in processing data right where it is generated, such as on our smartphones or smartwatches. This approach, known as edge computing, results in fewer travels to distant data centres, which might pose a security concern Ultimately, global collaboration may make a significant effect. Companies might share information about hazards and solutions, similar to neighbours keeping an eye on one other's houses. If everyone agrees on fundamental

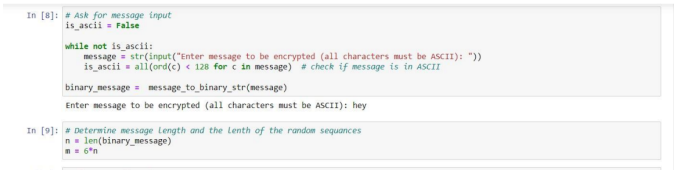

Fig. 5. Encrypted the message

safety guidelines for creating and using devices, we can build a safer environment for all of our linked devices. IoT-based solutions are already being used by several industries to develop new and/or significantly better technologies. IoT tools have been utilised in the medical field, for instance, allowing doctors to successfully monitor patients remotely and deliver medications based on data obtained from the hospital's IoT environment. IoT is widely regarded as the biggest frontier for enhancing humanity in a variety of ways, and it is safe to say that nothing in the history of information technology has had a greater impact on humanity than the IoT. Using Artificial Intelligence (AI) for Better Security: AI, or artificial intelligence, has become an important component of modern technology. Its potential will really appear when included with IoT security. AI, at its foundation, replicates human brain functions like learning and problem solving, but on a much bigger scale and at much faster rates. We can train our security systems to recognise patterns of possible attacks by utilising AI's deep learning capabilities. As the system meets more data, its knowledge improves, allowing it to forecast possible risks and act on them proactively. Furthermore, manually controlling a broad number of networked devices might be challenging. We can automate this procedure using AI.

Using Quantum Computing for Stronger Locks on Data: Quantum computing is an interesting technological area. Bits (0s and 1s) are used in traditional computers, while quantum computers employ quantum bits, also known as or qubits. This distinction enables quantum computers to process massive volumes of data at the same time. When it comes to encryption, the results are remarkable. While current encryption methods are robust, they might potentially be cracked with enough time and processing power. Quantum encryption, on the other hand, provides a new kind of security. Any unauthorised attempt to access the data with quantum keys affects the data itself, making breaches readily obvious. As we become more dependent on IoT devices, and these gadgets handle more sensitive data, the security provided by quantum computing becomes not only preferred, but necessary. Using Edge Computing to Keep Data Close: The edge computing idea is both beautiful and practical. In the past, an IoT device would send its data to a centralised server or cloud for processing. Not only does this use bandwidth, but it also creates a delay (latency) and significant security issues. The current model is turned on its head by edge computing. Instead of transferring data to a third party for processing, the computing takes place on the device itself, whether it's a security camera, a smart thermostat, or a wearable health monitor. This localised processing assures real-time data analysis, decreases network resource strain, and, most importantly, reduces the points of risk where hackers may intercept the data. Edge computing, in essence, makes IoT devices smarter, quicker, and more secure.

Working Together Worldwide for Better Safety: IoT security presents global concerns that must be addressed together. While individual businesses may and do adopt security measures, working together multiplies their efforts immensely. Consider a worldwide network where organisations may share information about the most recent dangers and responses. Because of this common information, a weakness uncovered in one part of the world may be promptly addressed in the rest. Furthermore, by establishing and implementing universal security standards, we can assure a baseline level of safety for all IoT devices, independent of origin or primary market. This worldwide cooperative structure assures that shared information and collective vigilance benefit the whole IoT ecosystem, from producers to end users. The decentralised, secure, and transparent aspect of blockchain technology, which makes information and privacy breaches challenging and even unachievable technically, is another reason why it is growing quickly. IoT solutions capacity to control how crucial information is shared and accessed, solutions employing blockchain can be developed to address the issues around information security and privacy at scale. Blockchain is already being tested and used in a number of sectors, and it is progressively coming to light as the crucial missing security link in the IoT ecosystem. Over time, it will become clear if it truly provides a consistent solution to the IoT's security and privacy issues. People use and see new smart devices every day that weren't around a few years ago, and many of these devices can communicate with one another without any problems from one side of the planet to the other. The result is that the world has.

METHODOLOGIES

It is critical to secure Internet of Things (IoT) devices and networks to avoid unauthorised access, data breaches, and potential disruptions. To improve IoT security, many techniques and best practises are used. Here are some examples of common methodologies: Device Authentication and Identity Management: Use robust authentication mechanisms such as Public Key Infrastructure (PKI) to ensure that only authorised devices can connect to the network. To avoid impersonation and unauthorised access, provide each device a unique identification and cryptographic key. Encrypt data in transit and at rest by employing secure protocols for communication such as Transport Layer Security (TLS) and strong encryption algorithms for data storage. Network Segmentation: Separate IoT devices into discrete networks to limit the potential impact of a breach and prevent attackers from moving laterally. Control and authorization of access: Apply the concept of least privilege by allowing just the essential access rights to IoT devices and users. To ensure that each person or device has the proper level of access, utilise role-based access control

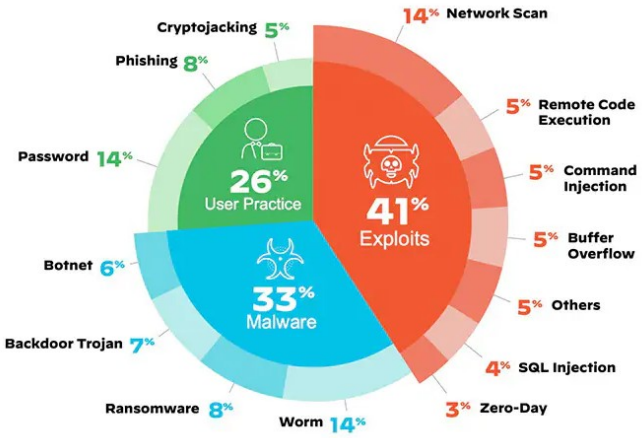

Fig. 6. Various Security issues

(RBAC). Anomaly Detection and Intrusion Prevention: Use intrusion detection and prevention systems (IDPS) in real-time to detect odd or malicious behaviour. Configure alarms to warn administrators of potential security breaches. Physical security measures include: To prevent unauthorised physical access to IoT devices, implement physical security measures. To safeguard electronics from physical attacks, consider tamper-evident packaging and anti-tampering features. Continuous Monitoring and Auditing: Use continuous monitoring to detect and respond to security incidents as soon as they occur. Conduct security audits and assessments on a regular basis to detect vulnerabilities and shortcomings. User Education and Training: Inform users and administrators on the hazards of IoT security, recommended practises, and how to identify potential threats such as phishing attempts. To effectively minimise threats and ensure the integrity of connected devices and networks, IoT security is an ongoing effort that necessitates a combination of technological protections, policies, and human awareness.

RESULT

The microprocessor is used to calibrate the values of the body temperature sensor, pulse rate sensor, room temperature and humidity sensor, and blood oxygen sensor. It is powered by an Arduino Uno and a handheld device. It collects all of the data from all of the detectors using an Arduino. Using a local server, they established a reading hub that was constantly updated. This technique was proposed to address concerns for the elderly and people who do not visit the doctor on a regular basis. Depending on the exact application and the kind of system employed, the outcomes of health monitoring systems can vary. Using health monitoring systems has led to the following outcomes, to name a few: The complete prototype of the health monitoring system with sensors is demonstrated, where the output values of the sensors are calculated and displayed in a linked device so that these results are visible even to the patient. Sensor values are shown on that device.

```
In [49]: # Encrypted messages can be send over classical chanel with unconditional security
         encrypted_message = encrypt_message(message, secret_key)

         print("The encrypted message is: " + encrypted_message)

         The encrypted message is: z0o

In [50]: # Bob can decrypt the messages with his copy of the secret key
         decrypted_message = decrypt_message(encrypted_message, bob_measured_values[:n])

         print("The decrypted message is: " + decrypted_message)

         The decrypted message is: hey
```

Fig. 7. Finally the message which is encrypted will be decrypted with same message with a lot of security using security key

These sensor readings are subsequently transmitted to the database server. Authorized users can access this data from the cloud using the IoT application platform.

The patient's sensor values are presented in the application. Sensor values are shown on the IOT Application Platform. Based on the information provided, the sickness of the patient is diagnosed by using the rules. The medical practitioner's assessment of one's health status. Even from a distance, the doctor can prescribe medications and recommend suitable actions.

CONCLUSION AND FUTURE WORK

IoT security is similar to a safety lock for our smart devices, and it is becoming increasingly vital as we use more connected devices. We're considering employing smart technologies like AI to improve these safety locks. AI can assist us by learning about new hazards and adapting our devices to protect us from them. We're also looking at tighter encryption ways to ensure that our private information remains secret no matter how sophisticated hackers get. Simultaneously, there is a significant shift towards managing data directly on our devices, such as smartphones, rather than transmitting it to remote computer centres. This makes it more difficult for hackers to gain access to our data. There's also talk of everyone working together on a global scale. Consider what would happen if all businesses exchanged information about possible risks; it would be like a neighbourhood watch for the digital world, making everything safer. Finally, as we include more smart gadgets into our homes and lives, it is critical to determine the best methods for keeping them secure. This includes utilising cutting-edge technology, collaborating, and ensuring that everyone understands how to use their gadgets properly.

REFERENCES

[1] Amin, F.; Abbasi, R.; Rehman, A.; Choi, G.S. An Advanced Algorithm for Higher Network Navigation in Social Internet of Things Using Small-World Networks. Sensors 2019, 19, 2007. [CrossRef] [PubMed]

[2] Patel, K.K.; Patel, S.M.; Scholar, P. Internet of things-IOT: Definition, characteristics, architecture, enabling technologies, application future challenges. Int. J. Eng. Sci. Comput. 2016, 6, 6122–6131.

[3] Hammoudi, S.; Aliouat, Z.; Harous, S. Challenges and research directions for Internet of Things. Telecommun. Syst. 2018, 67, 367–385. [CrossRef]

[4] Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Gener. Comput. Syst. 2013,29, 1645–1660. [CrossRef]

[5] Taherdoost, H. Blockchain-Based Internet of Medical Things. Appl. Sci. 2023, 13,1287. [CrossRef]

[6] Chaudhary, S.; Johari, R.; Bhatia, R.; Gupta, K.; Bhatnagar, A. CRAIoT: Concept, review and application (s) of IoT. In Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019; pp. 1–4.

[7] Survey paper on The Internet of Things: A survey Luigi Atzori DIEE, University of Cagliari, Italy, Antonio Iera University "Mediterranea" of Reggio Calabria.2010- Elsevier

[8] T. K. Jaimon, L.C. Katrina, G. Enying, and C. Paul, "The internet of things: Impact and implications for health care delivery," Journal of Medical Internet Research, vol. 22, no. 11, November 2020.

[9] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of things is a revolutionary approach for future technology enhancement: A review," Journal of Big Data, no. 111, 2019.

[10] L. Stephan, S. Steffen, S. Moritz, and G. Bela, "A review on blockchain technology and blockchain projects fostering open science," Journal of Frontiers in Blockchain, vol.2, p. 16, 2019.

[11] J. Chin, V. Callaghan, and S. B. Allouch, 'The internet-of-things: Reflections on the past, present and future from a user-centred and smart environment perspective," Journal of Ambient Intelligence and Smart Environments, vol. 11, 2019, pp. 45–69, DOI 10.3233/AIS180506.