ENHANCE SECURITY SYSTEM WITH THE USE OF INTERNET OF THINGS (IOT)

Bhawna Garg
Research Scholar
hibhawna21@gmail.com
Electronics and Communication Engineering
University of Technology, Jaipur

Raghavendra Patidar
Professor
raghvendrapatidar@gmail.com
Electronics and Communication Engineering
University of Technology, Jaipur

Abstract: The Internet of Things (IoT) is a dynamic, ever-changing ecosystem. enhancing security systems through the use of IoT and encryption techniques holds immense potential for improving the overall security and resilience of connected environments. By integrating IoT devices, networks, and encryption protocols, researchers and practitioners can bolster security measures, safeguard sensitive data, and mitigate risks associated with IoT deployments. This article explored various aspects of enhancing security systems with IoT and encryption techniques, outlining their benefits, implementation approaches, and future scope. The paper began by highlighting the benefits of incorporating IoT into security systems, emphasizing real-time data gathering, process automation, and remote monitoring capabilities. Internet-connected sensors and gadgets from the Internet of Things provide security systems the capacity to monitor for motion, analyze data, and identify people. track assets, and monitor environmental factors. Additionally, IoT integration enables remote access control, intrusion detection, and enhanced emergency response systems, all of which contribute to a comprehensive and efficient security framework. However, while IoT brings numerous advantages, It also opens up new entry points for attacks from bad actors. To counteract these risks, encryption techniques play a crucial role. The article explained how encryption can enhance security by protecting sensitive data, ensuring secure communication between devices, and establishing a robust security posture. This article suggested investigating machine learning for anomaly detection, developing comprehensive security frameworks for the entire IoT ecosystem, advancing threat intelligence and analytics systems, and working towards standardization and interoperability in IoT security. Finally, this thesis, enhancing security systems with IoT and encryption techniques presents significant opportunities to fortify the security and resilience of connected environments. By leveraging IoT capabilities and implementing robust encryption protocols, researchers and practitioners can address emerging challenges, safeguard data, and enable secure communication within the IoT ecosystem. With ongoing advancements and further research in this field, the future holds immense potential for innovative security solutions that will drive the safe and widespread adoption of IoT technologies across various industries and domains.

Keywords: IoT, Motion Sensors, Detectors, Biometric Authentication, Machine Learning, AI

I. INTRODUCTION

Enhancing a security system with the use of the Internet of Things (IoT) can significantly improve its effectiveness and responsiveness. IoT technology enables various devices to communicate with each other and the central system over the internet, creating a smart and interconnected security ecosystem [1][2][3]. Below are several ways we can leverage IoT to enhance our security system:

- **Smart Surveillance Cameras**: Replace traditional CCTV cameras with smart surveillance cameras equipped with IoT capabilities. These cameras can automatically detect motion, recognize faces, and provide real-time video feeds to security personnel or homeowners. Additionally, they can be integrated with other devices like door sensors and alarms.
- **Motion Sensors and Detectors**: IoT-enabled motion sensors and detectors can be placed strategically around the premises. They can detect any unusual movement or activity and trigger alerts or alarms.
- **Smart Locks and Access Control**: Upgrade traditional locks to IoT-enabled smart locks. These locks can be remotely controlled through a smartphone app and can also provide access logs, allowing homeowners or security personnel to monitor entries and exits.
- **Biometric Authentication**: Implement biometric authentication systems using IoT devices, such as fingerprint scanners or facial recognition cameras, to add an extra layer of security for access control.
- **Environmental Sensors**: IoT sensors can detect changes in environmental conditions like temperature, humidity, or gas levels. These sensors can help identify potential fire hazards or gas leaks and promptly notify the relevant authorities.
- **Alarm Systems**: Connect alarm systems to IoT devices, such as door/window sensors and motion detectors, to ensure immediate alerts in case of a breach.
- **Remote Monitoring**: IoT allows security personnel or homeowners to monitor the security system remotely through a smartphone or computer. This enables real-time access to surveillance feeds and the ability to control various security devices from anywhere.
- **Machine Learning and AI**: Combine IoT with machine learning and AI algorithms to analyze patterns and detect anomalies in the data collected by various sensors. This can help in predicting potential security threats and preemptive actions.
- **Cloud-Based Storage and Backup**: Store security footage and data on the cloud for redundancy and easy access. Cloud storage also ensures that critical evidence is not lost even if the local devices are compromised.
- **Automated Response Systems**: Use IoT devices to create automated response systems. For instance, if a security breach is detected, IoT can trigger a series of predefined actions, such as turning on lights, sounding alarms, or contacting emergency services.
- **Secure Communication Protocols**: Ensure that all communication between IoT devices and the central system is encrypted and secure to prevent unauthorized access or data breaches.
- **Regular Updates and Patches**: Keep all IoT devices and software up to date with the latest firmware and security patches to minimize vulnerabilities.

By integrating IoT technology into our security system, we can create a more proactive, interconnected, and responsive environment that enhances the overall safety and protection of our property. However, it's crucial to conduct thorough security assessments and regularly test the system to identify and address any potential weaknesses or vulnerabilities [4][5][6].

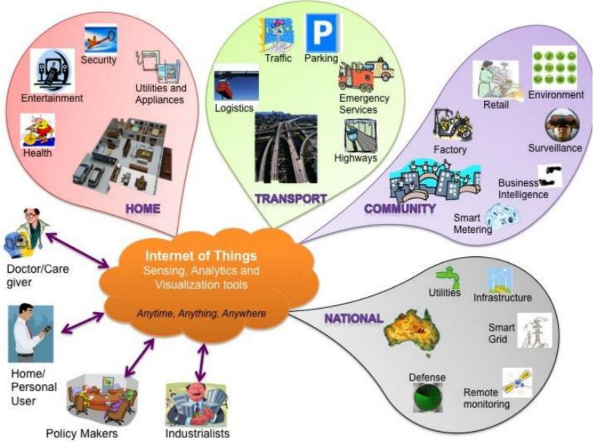


Fig. 1: Internet of Things Schematic showing the end users and application areas based on data

IoT Characteristics

Since many IoT devices have sensors and are capable of sophisticated data analysis, they are sometimes referred to as "smart." Internet-of-Things devices include sensors that gather information and then provide services to the user depending on that information and their preferences. Using sensors (such as cameras) to keep track of what's in the fridge and analyse that data using image recognition software, a smart fridge, for instance, might send a notification to the owner when certain perishables are running short. High-end IoT gadgets "learn" by analysing patterns in data about their owners' preferences and past use. An IoT device may get “smarter” when its software adapts to increase its prediction capabilities so as to boost user experiences or usefulness.

IoT devices are linked to the internet: directly, via another IoT device, or both. Network connections are utilised for exchanging information and connecting with people. The IoT develops links and connections between physical objects by adding software applications. Internet-of-Things devices allow users to view data or remotely operate gadgets from any location, using any device with an internet connection. For example, a smart doorbell and lock may enable a user to view and engage with the person at the door and open the door from anywhere using a mobile device or computer[7][8][10].

IoT Categories

There is a wide variety of applications for Internet of Things devices. In this part, we'll take a look at a few specific types of Internet of Things that often get the attention of lawmakers.

The industrial sector has started adopting commercial IoT applications, a trend known as the Industrial Internet of Things (IIoT). Industrial Internet of Things (IIoT) refers to the interconnection and communication of devices in a manufacturing setting with the purpose of enhancing performance, productivity, and efficiency. Providing real-time production data to detecting corrosion within a pipe at a refinery are just two examples of the wide range of uses for IIoT. Although there are now more consumer IoT connections than IIoT connections in North America, this may change in the near future. Industries such as manufacturing, chemicals, food and beverage, automotive, and steel stand to benefit greatly from the implementation of IIoT. The merger of IIoT and analytics is seen by experts as the Fourth Industrial Revolution, or 4IR.

Internet of Medical Things (IoMT): The healthcare profession has started adopting IoT, establishing the Internet of Medical Things (IoMT) (IoMT). Devices like heart monitors and pacemakers transmit patient health data to doctors and hospitals via the internet for analysis and adjustments to be made remotely. At a personal health level, wearable IoT devices, such as fitness trackers and smart watches, may monitor a user’s physical activity, basic vital statistics, and sleeping habits. According to a 2019 poll by Pew Research, nearly one-in-five Americans uses a smart watch or fitness tracker.

Smart Cities: IoT devices and systems in the utilities, transportation, and infrastructure sectors may be classified under the heading of “smart city.” Utilities may utilise IoT to develop “smart” grids and metres for electricity, water, and gas, where sensors gather and exchange consumer consumption data. With this information, the control system can better adjust output and distribution in response to fluctuations in demand. Transit IoT allows cities to implement fare readers and status trackers or locators that work with several modes of public transportation. Example: Columbus, Ohio's winning proposal for the 2016 Smart City Challenge from the Department of Transportation included a common payment and trip planning system across multiple transit systems and connected infrastructure that interacts with vehicles (such as electric autonomous vehicles and shuttles).

Smart appliances, TVs, entertainment systems, thermostats, light bulbs, outlets, door locks, door bells, and home security systems are all examples of consumer IoT devices often seen in "smart home" setups. All of these Internet-of-Things gadgets for the modern house may be linked together into a unified system and managed from anywhere with an internet connection and a computer or mobile device[9][10].

IoT Market Growth

According to Mordor Intelligence, the Internet of Things industry was $761.4 billion in 2020 and is projected to grow to $1.39 trillion by 2026.

IoT technology has been applied in many different industries, including manufacturing, retail, and healthcare, to monitor the spread of disease and manage the logistics of responding to a pandemic.

When edge computing and 5G networks become more widely available, IoT will be more accessible for business growth and expand at a quicker pace. Future smart factory automation using IoT technology will be possible thanks to this infrastructure, which will also support Industry 4.0, the continuing contemporary industrial revolution focused on automating production processes.

Selected Policy Issues

Congress may adopt IoT-related legislation and/or oversight activities. Challenges include include legislation, digital privacy, and data security among other policy issues.

Selected Policy Issues: Legislation and/or oversight pertaining to the Internet of Things may be taken by Congress. Challenges include include legislation, digital privacy, and data security among other policy issues.

Regulatory Issues: Emerging and converging technologies, such as IoT, may not accord entirely with federal agency supervision powers. A newly formed framework may leave certain aspects of new technology uncontrolled, partly regulate them, or regulate them more thoroughly. Many consumer IoT devices are already allowed to self-regulate by the industry. Policies for deconfliction, harmonisation, and/or enlargement of agency jurisdictions may be required for federal regulation of IoT.

Digital Privacy Issues: With the advent of the Internet of Things, there is a greater opportunity for data gathering and use, which might raise privacy issues. Identify, find, track, or monitor an individual without their knowledge might be accomplished with even a small portion of the obtained data. It's possible to take advantage of the disclosed patterns in their actions. The challenge arises from the fact that protecting users' private data online and developing cutting-edge technology like the Internet of Things (IoT) may be incompatible. Although more widespread data gathering and analysis has the potential to boost productivity, efficiency, and creativity, it also poses risks of compromising personal information and being used in ways that users have not approved.

Regulatory Issues: The authorities of government agencies charged with keeping an eye on things may not always line up with the needs of rapidly evolving and converging technologies like the Internet of Things. A newly formed framework may leave certain aspects of new technology uncontrolled, partly regulate them, or regulate them more thoroughly. Many consumer IoT devices are already allowed to self-regulate by the industry. Policies for deconfliction, harmonisation, and/or enlargement of agency jurisdictions may be required for federal regulation of IoT.

Regulatory Issues: The authorities of government agencies charged with keeping an eye on things like the Internet of Things (IoT) may not always mesh with the realities of these rapidly developing technology. Any number of different regulatory approaches may be taken toward emerging technology depending on the specifics of the framework in place. Many consumer IoT devices now operate under this industry-led self-regulation model. Deconfliction, harmonisation, and/or extension of agency jurisdictions may be part of the federal government's plans for regulating the Internet of Things (IoT).

Internet of Things (IOT) in Security System

The Internet of Things (IoT) has revolutionized various industries, including security systems. IoT in security systems refers to the integration of smart devices, sensors, and other connected technologies to enhance the overall security and safety of homes, businesses, and public spaces. Here are some key aspects of IoT in security systems:

- Smart Surveillance Cameras: IoT-enabled surveillance cameras are equipped with advanced features like high-definition video recording, motion detection, facial recognition, and remote access. These cameras can be connected to the internet and allow users to monitor their property in real-time through smartphones or computers.
- Home Automation and Security: IoT technology allows homeowners to automate various security processes, such as remotely controlling door locks, setting up smart alarms, and monitoring sensors for unauthorized entry. This provides users with greater control and peace of mind regarding their home security.
- Sensor Networks: IoT-based security systems use a network of sensors (e.g., motion sensors, door/window sensors, smoke detectors) that can communicate with each other and the central monitoring station. These sensors can trigger alarms or notifications in case of any suspicious activities or emergencies.
- Access Control: IoT has improved access control systems by incorporating biometric authentication, keyless entry, and remote access management. Users can grant access to specific individuals, track entry logs, and receive alerts when someone attempts unauthorized access.
- Data Analytics and AI: With the integration of data analytics and artificial intelligence (AI), IoT security systems can process vast amounts of data and identify patterns or anomalies that might indicate potential security threats. AI-driven algorithms can also learn from past events and improve the system's ability to detect suspicious behavior.
- Cloud-Based Storage and Remote Monitoring: IoT security systems often use cloud-based storage to store surveillance footage and other data. This allows users to access the data from anywhere with an internet connection, providing flexibility and convenience for remote monitoring.
- Enhanced Integration: IoT enables the integration of various security devices and systems, creating a comprehensive security ecosystem. For instance, integrating security cameras with alarm systems, access control, and environmental sensors can enhance overall security and emergency response capabilities.
- Scalability: IoT-based security systems are often scalable, allowing users to expand their security setup easily. New devices can be added to the existing network without significant disruptions or changes to the infrastructure.

However, while IoT brings numerous benefits to security systems, it also raises concerns about data privacy, cybersecurity, and potential vulnerabilities in interconnected devices. Therefore, it's crucial for manufacturers and users to implement robust security measures, regular updates, and best practices to mitigate potential risks and ensure a safe and secure IoT-based security system[11][12][13][14].

II. RESEARCH METHODOLOGY

The Internet of Things (IoT)

This mechanism enabled systems in the healthcare sector have performed remote monitoring, releasing the potential to preserve patient safety and health and enabling doctors to offer the best possible quality of treatment. With a simpler and more efficient contact with physicians, patient health and happiness also increase. Furthermore, remote health monitoring may reduce hospital stays and avoid re-admission. The IOT may potentially have a significant effect on medical expenditures and treatment results. By rethinking device space and interactions between people, IOT changes the healthcare sector. IoT application is beneficial to patients, families, physicians, hospitals, and insurance companies in the area of medicine. The public has now captured the eye of reports that call attention to internet computer theft, security issues, and privacy concerns. New political, legal and growth problems are emerging and technological obstacles remain. This summary paper is meant to help the Internet population tackle the Internet of Things controversy in the face of conflicting assumptions about its commitments and threats. From multiple viewpoints, the Internet of Things contains a broad variety of nuanced and interwoven concepts. The core principles that act as a framework for exploring possibilities and obstacles for IoT include:

Enabling technologies: The concept of integrating machines, cameras, and networks for the purpose of system tracking and control has been kicking around for several decades. The Internet of Things, on the other hand, is getting closer to being a reality of the mainstream as a result of the recent integration of various developments in the technology industry. This includes the widespread deployment of IP-based networks, advances in data mining technology, miniaturisation of computing components, computing economics, and the expansion of cloud storage and computing services.

Communication forms: IoT applications make use of a wide variety of technological contact models, each of which possesses its own set of characteristics. It makes use of the four traditional communication models defined by the Internet Engineering Board (IEB), which are device-to-device, device-to-cloud, device-to-gateway, and sharing of background data. These models exhibit a high degree of versatility in terms of the ways in which Internet of Things devices can communicate with one another and provide the user with benefits.

Transformational potential: If IoT hopes and patterns came true, it might force a change in thought about the consequences and challenges in an environment where passive sharing of linked artefacts rather than constructive content participation is the most prevalent contact with the Internet. Although security issues in the IT sense are not fresh, the interfaces of many IoT apps raise different and unusual challenges to protection. It must be a high priority to face these obstacles and maintain the protection of IoT goods and services. Users must trust that, especially as this technology becomes usable, IoT devices and related data resources are secure from security vulnerabilities. In our everyday lives, it is becoming more widespread and incorporated. Poorly secured IoT devices and services will serve as possible entry points for cyber-attacks and, by leaving data flows insufficiently covered, expose user data to theft. The embedded existence of IoT devices ensures that any weakly secured system connecting to the Internet can have a global effect on the Internet's protection and resilience. Other aspects.

In practice, manufacturers, and consumers of IoT devices and applications are under a collective duty to guarantee that no potential damage is caused to consumers or to the Internet. Therefore, to create efficient and acceptable responses to IoT security issues that are completely proportional to the scale and severity of the problems, a collective approach to security would be needed. The Internet of Things was the first major networks in the 21st century. Real-life events are part of the Internet with their computer and networking capabilities and enabling them to communicate with other IoT devices. By improving the Internet of Things, the web theory is expanding and advancing. Seamless communications between different device types, like home devices, medical sensors, vehicles, surveillance cameras, etc. Many applications have been developed in the IoT world, including home automation, the smart city, traffic management, an intelligent network, health security and data protection patients.

IoT solutions for the health industry from the Body Sensor Network (BSN). This is a group of small, lightweight wireless sensor nodes for tracking the functions ruthless operations, extensive security measures are needed to avoid malicious system interactions. The Internet of Health IoT is still in its infancy in terms of modeling, implementation and growth, but the application of the Internet of Things has had a significant impact and is driving the demand for today's healthcare industry and health management solutions based on the Internet of Things. In the United States, the Internet of Things will protect 50,000 people from medical errors this year. According to research, the Internet provides better treatments at cheaper costs in the healthcare sector, reduces direct interaction between workers. This artefact is a continuation of the data preservation strategy of the Health Internet of Things. The cognitive layer is primarily responsible for collecting health data from a variety of sensors. The network layer consisting of a wireless device and intermediary processes and transmits information received through a sensitivity layer of the application platform. There are no changes to well-designed transport protocols[15][16][17].

IoT Platform

The IoT framework is a multi-layered technology that allows linked devices inside the IoT environment to be conveniently provided, controlled, and automated. Basically, utilizing scalable connation choices, enterprise-grade authentication protocols, and extensive data-processing powers, it links the computers, no matter how diverse, to the cloud. The IoT framework provides developers with a collection of off-the-shelf features that significantly speed up the creation of apps for connected devices, as well as paying attention to scalability and product usability. Therefore, depending on the way we look at it, the IoT platform may have various functions. When we speak of how remote machines link to user apps (or other machines) and handle all communications between hardware and application levels, it is usually referred to as middleware. In order to describe the core market value, which is the traditional hardware empowerment of cloud-based software and services, it is often regarded as the cloud enablement framework or Internet of things enablement framework. Finally, it changes the emphasis to becoming a key support for IoT developers under the name of the IoT Device Enablement Framework.

IoT Platform Technology Stack

A sophisticated IoT framework can provide we with much of the IoT functionality necessary to build our connected devices in the standard four layers of an IoT stack, including stuff, networking, simple IoT features, apps and analytics. And insightful things. Our computers link, either directly or via an IoT portal, to the cloud network or our local data center. When the endpoints do not connect directly in the cloud or, for example, require any edge computing resources, a gateway comes in handy. For eg, when our endpoints are on the Lora Wan network, however we need them to connect with the cloud through MQTT, we may also use the IoT gateway to convert protocols. We can break the IoT platform itself into several layers. The infrastructure level is at the bottom, which is something that helps the network to run. Container control components, on-premise platform messages, IoT suite harmonization, and more can be found here. In other terms, this is when computers link to the cloud to execute different operations; the networking layer helps messages to be transmitted to computers.

The next layer illustrates the primary IoT features supported by the framework. The basics include data processing, system control, and management of setup and communications, and app upgrades for OTA. There is another dimension that is less relevant to the sharing of data between devices than to the processing of that data on the network. There are reports that make it easy to build personalized reports for you. In user programmers, there is a simulation of data representation. Then there is the engine for regulations, analytics, and warnings to inform we about any observed irregularities in our IoT solution. Most notably, this can incorporate industry-specific components and third-party apps with the best IoT platforms. Without this versatility, there may be a substantial added expense to build an IoT platform for a particular market situation and postpone the delivery of the solution indefinitely.

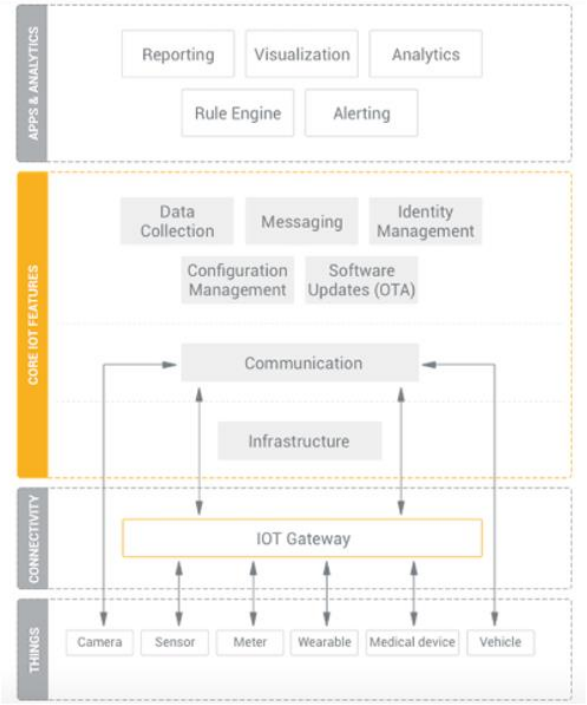


Fig. 2: IoT Platform Technology Stack

Advanced IoT platforms

Other critical factors, such as scalability, customization, ease of usage, power over code, collaboration with third-party applications, deployment choices, and data protection standard, differentiate IoT systems from each other.

- **Scalable (cloud native)** – The sophisticated IoT systems guarantee scalable scalability through any number of endpoints a consumer may need. For public cloud implementations, this feature is taken for granted, but can be evaluated explicitly for on-site implementation, including load-balancing functionality for the platform to improve the efficiency of the server cluster.
- **Customizable** – A vital variable for distribution speed. Good APIs may be appropriate for aviation for tiny and lenient IoT solutions, whereas feature-rich and quickly changing IoT environments.
- **Secure** –Protection of data includes confidentiality, end-to - end control of identities, and scalable implementation. End-to - end data flow encryption, including insecure data, system verification, management of user access privileges, and confidential data private cloud resources-these are the fundamentals of how to protect the IoT approach from breaching breaches.

Application

Fingerprint Scanners using the IoT sensor

There are three types of fingerprint scanners: **optical, capacitive,** and **ultrasound.** In this case, an optical scanner captures a snapshot of the finger, recognizes the print pattern, and then combines the information into an identifying code.

- It is possible to use a capacitive scanner to detect electrical impulses sent from a finger to the scanner. The print ridges immediately contact the scanner, transferring electrical current, whilst the valleys between the print ridges generate air gaps, allowing for more efficient printing. A capacitive scanner essentially maps out these contact sites and air gaps, resulting in a pattern that is completely unique to the scanner's user. These are the types of chips that are found in smartphones and computers.
- Scanners that use ultrasonic waves will be included in the next generation of smartphones. To put it simply, they will emit ultrasounds that will reflect back into the scanner. Similar to a capacitive sensor, it creates a map of the finger that is unique to the user.

Fig. 3: Biometric Authentication Methods

Biometric Authentication using IoT sensor

Biometrics has long been the aim of future authentication, with the expectation that it will substantially replace existing present identification and access control methods. Biometric systems may be utilized in two ways.

• **Verification (1–1):** verifying a person's identity. In verification mode, the system verifies the person's identity by comparing biometric data to a database template.

The person's identity is determined (1-n). In identification mode, the system looks up the person's template in the database.

Basically, a biometric system works by collecting biometric data from a person, extracting features from the data, and comparing them to the database template.

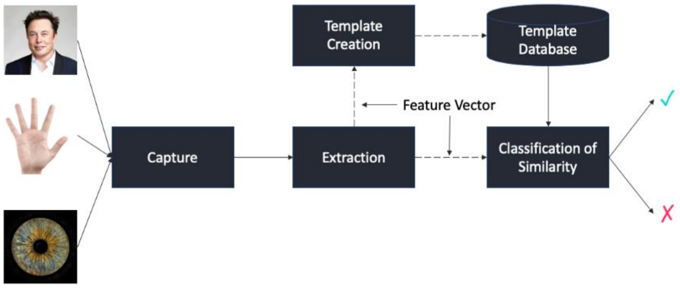


Fig. 4: Biometric System

Biometric Methods

Biometrics, or unique human features, have been used for hundreds of years in various forms, including physical descriptions and more recently photographs. Physiological or behavioral peculiarities are considered in biometric authentication.

Biometrics Physiology

Physiological biometrics uses data from the human body to identify a person, such as fingerprints, face, or iris.

Fingerprint ID

The fingerprint identification system, which is the most frequently used biometric to date, employs a number of categorization techniques based on minutiae, which are epidermal friction ridges found on the palm side of fingers and thumbs, as well as on the palms and soles of feet. They may be used for authentication purposes in accordance with the following concepts.

- A fingerprint does not change over time.
- Fingerprints feature typical ridge patterns that allow classification.
- A fingerprint is unique because no two fingers have the same ridge pattern.

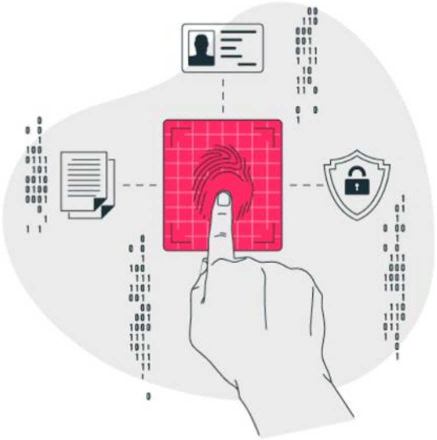


Fig. 5: Fingerprint ID

Hand Shapes

Hand geometry is the second most popular biometric. The geometric properties of the hand, such as finger lengths and hand breadth, are used to identify people.

Face-reading

The device captures facial photos with a digital video camera and analyses **them for features including eye, nose, mouth, and jaw distance.**

Iris Detection

Parts of the human eye are shown below.

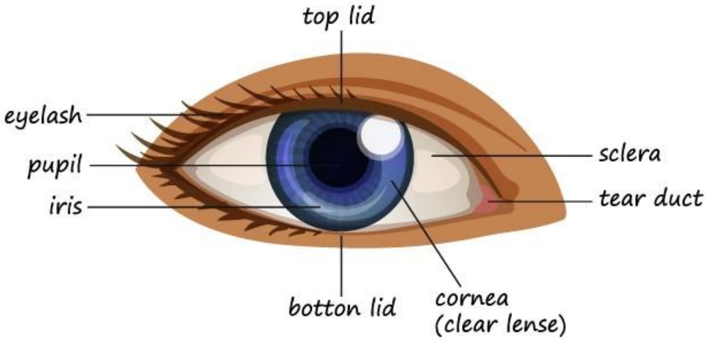
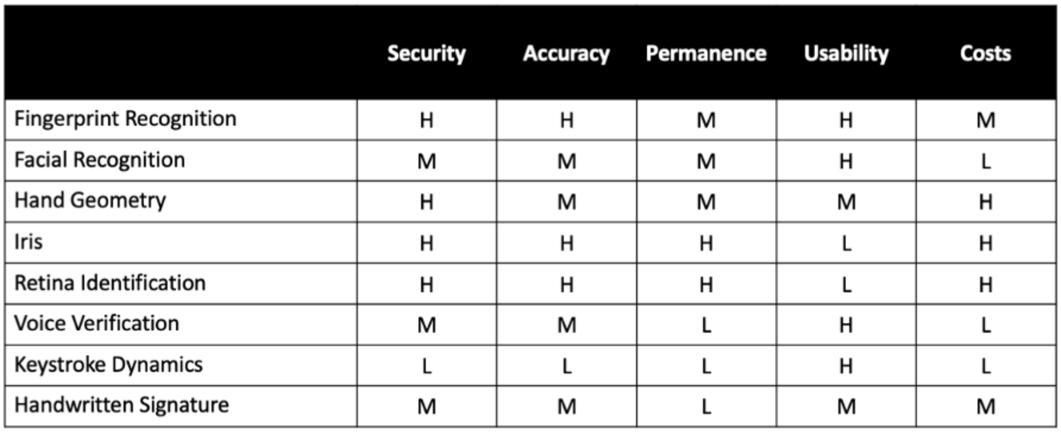


Fig. 6: Iris Detection

The iris is the colorful tissue around the pupil of the eye.

The table below compares the biometric types discussed in this research.

Table 1: compares the biometric types



	Security	Accuracy	Permanence	Usability	Costs
Fingerprint Recognition	H	H	M	H	M
Facial Recognition	M	M	M	H	L
Hand Geometry	H	M	M	M	H
Iris	H	H	H	L	H
Retina Identification	H	H	H	L	H
Voice Verification	M	M	L	H	L
Keystroke Dynamics	L	L	L	H	L
Handwritten Signature	M	M	L	M	M

Techniques of biometric authentication

Accuracy

Because data collection environments and biometric scanners vary, it is impossible to obtain 100% accuracy. Thus, reliable biometric technology requires specific performance standards. The FAR and the FRR are the two commonly utilized biometric performance measurements.

- **High accuracies:** fingerprint, iris. Accurate face, hand geometry, signature and voice.

High speed: keystroke dynamics

Permanence
The biometric should not alter over time.

- **Longevity:** fingerprint, face, hand geometry
- **Longevity:** iris, retina.
- **Impermanence:** voice, keystrokes, and handwriting

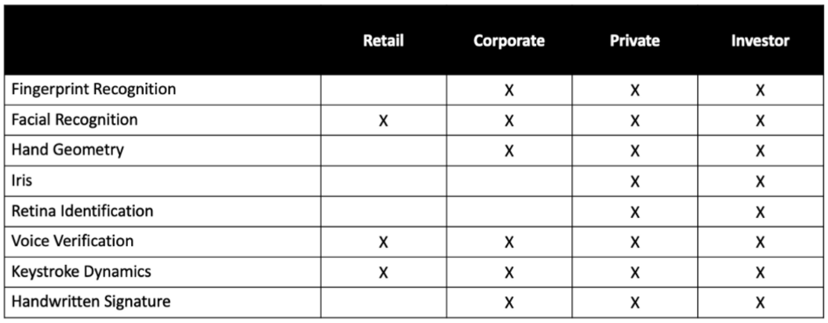
Usability
Being user-friendly and responsive to user demands
Biometric, face, keystroke and voice recognition.

- **Usability:** hand geometry and signature
- Iris and retinal: unusable

Costs
Technical expenses, such as installation and maintenance, in the total authentication system. Ink, iris, retinal and handwritten signatures are costly.

- Fingerprint:

Affective dynamics of the face & voice
Adequacy
Ability to suit the demands and expectations of a certain user category (retail, corporate, private, or investment).
Table 1: user category Authentication retail, corporate, private, or investment



	Retail	Corporate	Private	Investor
Fingerprint Recognition		X	X	X
Facial Recognition	X	X	X	X
Hand Geometry		X	X	X
Iris			X	X
Retina Identification			X	X
Voice Verification	X	X	X	X
Keystroke Dynamics	X	X	X	X
Handwritten Signature		X	X	X

The user segment of the biometric authentication technique

Biometrics Hacked
Replay attacks
In a replay attack, an intruder captures successful biometric login sessions and then attempts to complete authentication on his own using the acquired data.

Faked credentials
Some biometric systems may be subject to credential forgery. For example, a hacker may deceive a biometric system that uses face recognition by presenting a life-size image of the person in front of the camera.

Stolen credentials
Biometric systems are subject to credential theft in different ways. But a stolen eye is horrible to us. A stolen larynx has yet to be utilized to effectively trick a voice-based biometric system, so we believe secure.

Database Construction for face detection biometric data security application

The first step is to create a database of information. We make use of the database to assess whether or not the person is authorised to enter the country. Face detection is a method for identifying and estimating the location of face landmarks in an image (e.g., eyes, nose, mouth, and cheek). Face detection is the challenge of recognising a person's face in a photograph.

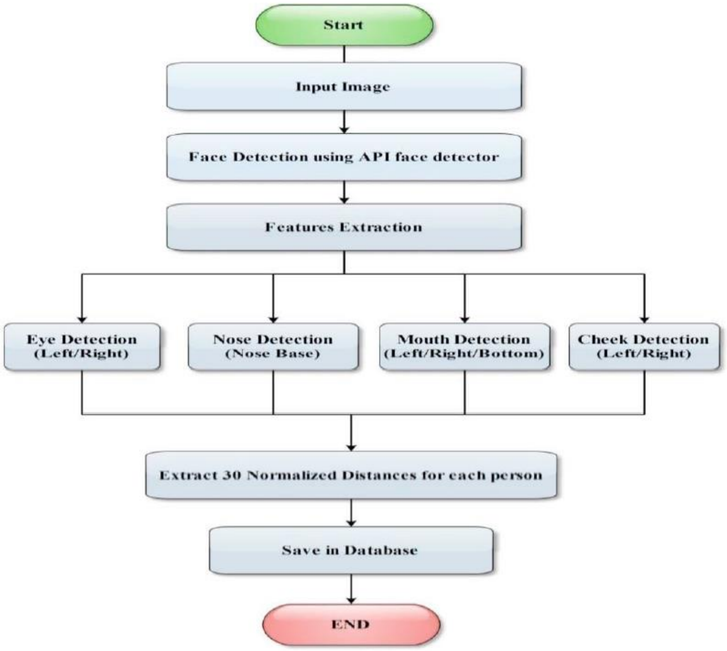

Start
Input Image
Face Detection using API face detector
Features Extraction
Eye Detection (Left/Right)
Nose Detection (Nose Base)
Mouth Detection (Left/Right/Bottom)
Cheek Detection (Left/Right)
Extract 30 Normalized Distances for each person
Save in Database
END

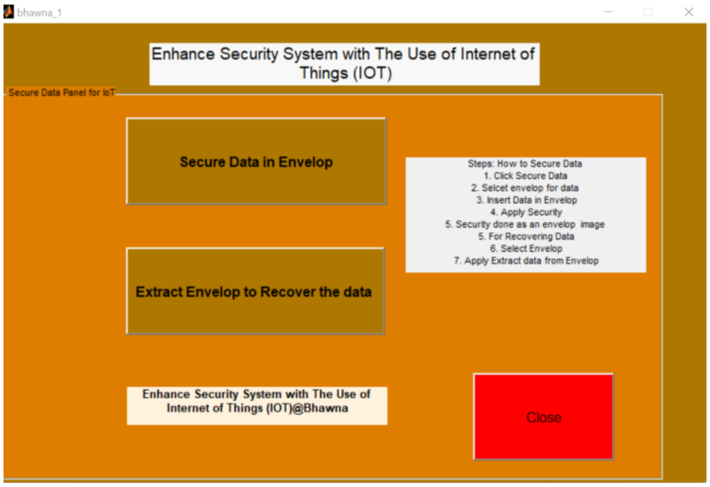
Fig. 7: Database Construction

III. SIMULATION AND RESULT

The Internet of Things (IoT) is a term that describes the billions of different physical devices that can be found all over the globe that are linked to the internet. These devices all gather and share data with one another. Despite this, a growing number of consumers are choosing not to use Internet of Things devices due to rising security concerns, such as software vulnerabilities and cyberattacks. Such Internet of Things security issues are especially significant for businesses operating in industries such as healthcare, finance, manufacturing, logistics, retail, and other fields that have already begun adopting IoT systems. These industries include retail, logistics, and supply chain management. The Internet of Things (IoT) is quickly gaining widespread adoption in recent years. The rapid expansion of the Internet of Things is being fueled in large part by the astonishingly cheap prices of various sensors. This technology is being progressively used in many other areas, including healthcare, construction, agriculture, and transportation, among others. When it comes to the future of the Internet of Things, however, security and privacy are two major problems that need to be addressed. This thesis mainly focusses on the study of the use of Use of Internet of Things (IOT)

Ensuring Public Data through

Apply security of data techniques for protecting the User data from unethical access over the IoT devices. For this we have used. According to what was discovered above, the data of users could be protected by encryption and recovered using the Euclidean Algorithm. This algorithm offers a security feature and makes it easier for people with diabetes to use devices connected to the internet of things.


bhawna_1
Enhance Security System with The Use of Internet of Things (IOT)
Secure Data Panel for IoT
Secure Data in Envelop
Extract Envelop to Recover the data
Enhance Security System with The Use of Internet of Things (IOT)@Bhawna
Close

Steps: How to Secure Data
1. Click Secure Data
2. Selcet envelop for data
3. Insert Data in Envelop
4. Apply Security
5. Security done as an envelop image
5. For Recovering Data
6. Select Envelop
7. Apply Extract data from Envelop

Fig. 8: basic GUI

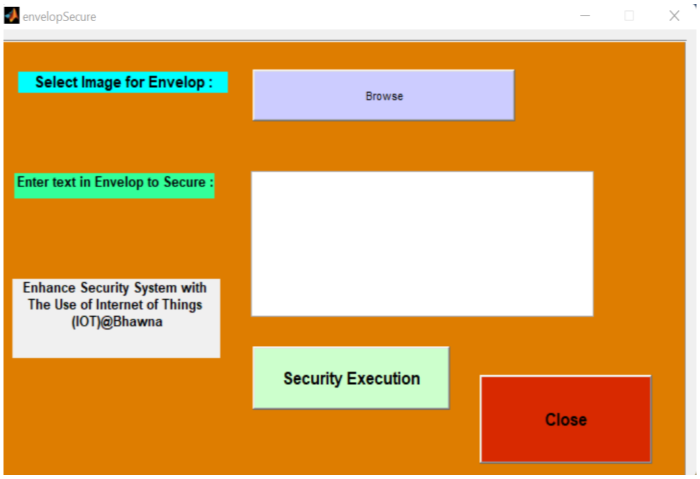
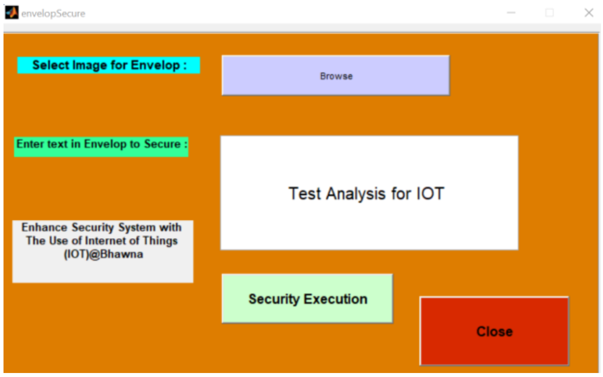

envelopSecure
Select Image for Envelop :
Browse
Enter text in Envelop to Secure :
Enhance Security System with The Use of Internet of Things (IOT)@Bhawna
Security Execution
Close

Fig. 9: Secure data

In Fig. 8, This is default GUI for securing the user data. This has two green executable buttons along with one exit button. The first green button has secure data in envelop and second green button has assigned as extraction from envelop.

In Fig. 9, This has one envelop for data security. This feature provides the safe guard to user data. As we know that the security has very important concern over the IoT devices. Beside the sensitivity of user data is also very important to secure from unauthentic activities. So, this security execution provides data transmission over the envelop.


envelopSecure
Select Image for Envelop :
Browse
Enter text in Envelop to Secure :
Enhance Security System with The Use of Internet of Things (IOT)@Bhawna
Security Execution
Close

Test Analysis for IOT

Fig. 10. Data insertion in envelop

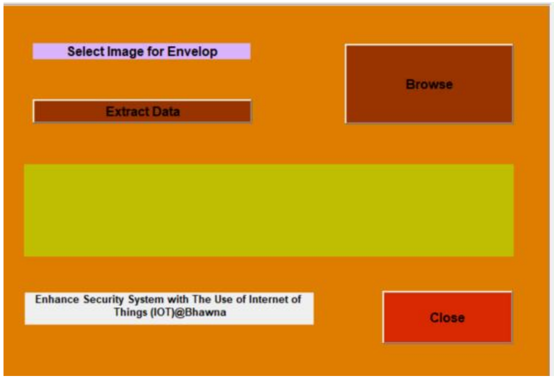

Select Image for Envelop
Browse
Extract Data
Enhance Security System with The Use of Internet of Things (IOT)@Bhawna
Close

Fig. 11: Extract data from envelop

In Fig. 10, For data security, there is only one wrap. This feature ensures the security of user data. As we all know, security is a major worry when it comes to IoT devices. As a result, this security execution allows data to be transmitted across the envelop. Further text inserts for transmission of data.

In fig, 11, Extract the transmission data from envelop and using the extract data button.

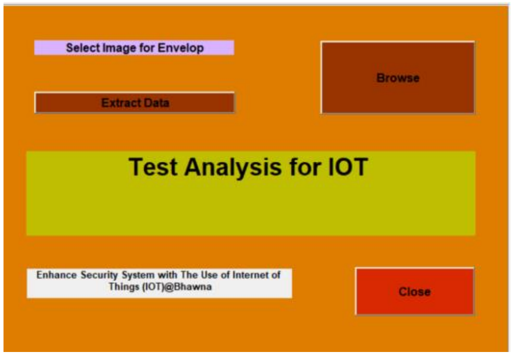

Select Image for Envelop
Browse
Extract Data
Test Analysis for IOT
Enhance Security System with The Use of Internet of Things (IOT)@Bhawna
Close

Fig. 12. Data extracted from envelop

The above fig. 12 presented the secure data again recovered and reflected in envelop. So, these processes secure the user data. This is the ultimate goal of this thesis.

IV. CONCLUSION AND FUTURE SCOPE

Enhancing a security system with the Internet of Things (IoT) offers numerous benefits. By leveraging IoT technologies, security systems can become more efficient, effective, and responsive. One key advantage is in smart surveillance, where IoT cameras and sensors provide intelligent monitoring capabilities. These devices can analyze movements, recognize faces, and send alerts for any suspicious activities, enabling proactive security measures. IoT also revolutionizes access control systems. It allows for remote management of access permissions, real-time tracking of entry and exit events, and access logs, providing enhanced control and monitoring. Intrusion detection is another area where IoT shines. Sensors deployed throughout a facility can detect unauthorized access or break-ins, promptly alerting the appropriate personnel for immediate action. Furthermore, IoT devices enable environmental monitoring, keeping tabs on factors like temperature, humidity, and air quality. This functionality helps prevent security breaches and potential damage by triggering alarms in the event of abnormal changes. Asset tracking is also made possible through IoT. By attaching RFID tags or GPS trackers to valuable assets, their real-time location can be monitored, and any unauthorized movement or tampering can be quickly identified. The wealth of data generated by IoT devices can be harnessed through analytics, allowing security professionals to gain valuable insights. Data analysis can identify security patterns, vulnerabilities, and even predict threats, leading to more effective response strategies. Additionally, IoT facilitates integration with other systems like fire alarms or building management systems, enabling a comprehensive and coordinated security approach. IoT empowers security systems with remote monitoring and management capabilities. Security personnel can access live video feeds, receive real-time alerts, and control various security devices through mobile applications or web interfaces, regardless of their physical location. Moreover, in the event of emergencies, IoT can be integrated with communication channels and emergency services, automating alerts and providing relevant data for faster response.

While IoT enhances security systems, it is crucial to implement robust security measures. Strong authentication, encryption, regular firmware updates, and network segmentation are essential to safeguard IoT devices and data from potential cyber threats. By embracing IoT technologies in security systems, organizations can significantly improve their overall security posture. In conclusion, the use of the Internet of Things (IoT) in enhancing security systems offers numerous benefits. By leveraging IoT technologies, security systems can become more efficient, effective, and responsive. Incorporating encryption techniques further strengthens the security of IoT systems by protecting sensitive data and ensuring secure communication between devices. Through the implementation of encryption algorithms in MATLAB, researchers can explore various cryptographic techniques such as symmetric and asymmetric encryption. By encrypting data during transmission and storage, the confidentiality and integrity of IoT data can be safeguarded. Researching the use of encryption in IoT security involves designing an IoT security architecture, implementing encryption algorithms, and evaluating their performance and security. Factors such as computation time, memory usage, and energy consumption need to be considered to ensure a balance between security and system efficiency. Additionally, addressing IoT-specific challenges like resource constraints and communication protocols is crucial in developing effective encryption solutions. By this thesis the research methodology, implementation details, and findings, researchers can contribute to the knowledge and understanding of how encryption techniques can enhance IoT security. The research outcomes can help organizations and practitioners in implementing robust security measures to protect their IoT systems from potential threats.

Overall, the use of encryption in IoT security research aims to provide insights into improving the resilience, confidentiality, and integrity of IoT systems, fostering trust and enabling the widespread adoption of IoT technology in various industries and domains.

Future Scope

The future scope of enhancing security systems with the use of IoT and encryption techniques is promising and offers several opportunities for further development and advancement. Here are some potential areas of future exploration:

Quantum Encryption: As quantum computing evolves, there will be a growing need for quantum-resistant encryption algorithms. Research can focus on developing and implementing post-quantum encryption techniques to ensure the long-term security of IoT systems.

Edge Computing Security: With the rise of edge computing in IoT, there will be a need for robust security measures at the edge devices. Future research can focus on developing lightweight encryption algorithms and protocols suitable for resource-constrained edge devices while maintaining a high level of security.

Blockchain Technology: Blockchain has gained significant attention in the field of IoT security. Research can explore the integration of blockchain with IoT systems to enhance security, immutability, and transparency. This includes investigating decentralized identity management, secure data sharing, and trust mechanisms.

Machine Learning for Anomaly Detection: Machine learning algorithms can be applied to IoT data streams for real-time anomaly detection and threat identification. Research can focus on developing advanced machine learning models that can adapt to evolving security threats and provide early detection of malicious activities.

Privacy-Preserving Techniques: IoT generates massive amounts of data, raising concerns about privacy. Future research can explore privacy-preserving encryption techniques, differential privacy, and secure data anonymization methods to protect sensitive user information while still enabling effective IoT system operation.

Security in IoT Ecosystems: As IoT systems become more complex and interconnected, research can focus on developing comprehensive security frameworks that address security challenges across the entire IoT ecosystem. This includes secure device onboarding, secure communication protocols, and secure integration with cloud platforms.

Threat Intelligence and Analytics: Research can focus on developing advanced threat intelligence and analytics systems specifically tailored for IoT security. This involves leveraging big data analytics, machine learning, and artificial intelligence techniques to identify emerging threats, predict attacks, and enable proactive security measures.

Standardization and Interoperability: As IoT devices and systems come from various manufacturers and operate on different protocols, research can contribute to developing standardized security frameworks and interoperability standards. This will ensure seamless integration and secure communication between different IoT devices and platforms.

The future scope of enhancing security systems with IoT and encryption techniques lies in addressing emerging challenges, exploring innovative approaches, and developing holistic security solutions to protect IoT systems and data. The continuous evolution of IoT technology and the increasing adoption of connected devices offer a fertile ground for research and development in the field of IoT security.

REFERENCES

1. Wang, J., Lim, M. K., Wang, C., & Tseng, M. L. (2021). The evolution of the Internet of Things (IoT) over the past 20 years. *Computers & Industrial Engineering*, *155*, 107174.
2. Javaid, M., & Khan, I. H. (2021). Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. *Journal of Oral Biology and Craniofacial Research*, *11*(2), 209-214.
3. Liu, L., Guo, X., & Lee, C. (2021). Promoting smart cities into the 5G era with multi-field Internet of Things (IoT) applications powered with advanced mechanical energy harvesters. *Nano Energy*, *88*, 106304.
4. Keserwani, P. K., Govil, M. C., Pilli, E. S., & Govil, P. (2021). A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model. *Journal of Reliable Intelligent Environments*, *7*(1), 3-21.
5. Bansal, M., Nanda, M., & Husain, M. N. (2021, January). Security and privacy Aspects for Internet of Things (IoT). In *2021 6th International Conference on Inventive Computation Technologies (ICICT)* (pp. 199-204). IEEE.
6. Song, T., Cai, J., Chahine, T., & Li, L. (2021). Towards smart cities by Internet of Things (IoT)—a silent revolution in China. *Journal of the Knowledge Economy*, *12*(2), 1-17.
7. Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*, *1*(1), 1-14.
8. Lv, Z. (2021). Security of internet of things edge devices. *Software: Practice and Experience*, *51*(12), 2446-2456.
9. HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2021). A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things*, *14*, 100129.
10. Islam, N., Rashid, M. M., Pasandideh, F., Ray, B., Moore, S., & Kadel, R. (2021). A Review of Applications and Communication Technologies for Internet of Things (IoT) and Unmanned Aerial Vehicle (UAV) Based Sustainable Smart Farming. *Sustainability*, *13*(4), 1821.
11. Smys, S., Basar, A., & Wang, H. (2020). Hybrid intrusion detection system for internet of Things (IoT). *Journal of ISMAC*, *2*(04), 190-199.
12. Tahsien, S. M., Karimipour, H., & Spachos, P. (2020). Machine learning based solutions for security of Internet of Things (IoT): A survey. *Journal of Network and Computer Applications*, *161*, 102630.
13. Singh, R. P., Javaid, M., Haleem, A., & Suman, R. (2020). Internet of things (IoT) applications to fight against COVID-19 pandemic. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, *14*(4), 521-524.
14. Al-Turjman, F., & Lemayian, J. P. (2020). Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: an overview. *Computers & Electrical Engineering*, *87*, 106776.
15. Nižetić, S., Šolić, P., González-de, D. L. D. I., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production*, *274*, 122877.
16. Mabodi, K., Yusefi, M., Zandiyan, S., Irankhah, L., & Fotohi, R. (2020). Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. *The Journal of Supercomputing*, 1-26.
17. Swamy, S. N., & Kota, S. R. (2020). An empirical study on system level aspects of Internet of Things (IoT). *IEEE Access*, *8*, 188082-188134.
18. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1646-1685.