iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79867

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

A Smart Review of Internet of Things Applications and Their Security Issues

Bishal Biswas[1], Subhankar Sarkar[2], Soumen Bhowmik[3]
[1]*M.Tech - CSE, Bengal Institute of Technology and Management, Santiniketan, Birbhum, West Bengal. India*
[2] *Ph.D. Enrolled - Department of CSE, MAKAUT, Simhat, Nadia, West Bengal. India*
[3]*Assistant Professor & HOD - Department of CSE, Bengal Institute of Technology and Management, Santiniketan, Birbhum, West Bengal. India*

Abstract: ***Internet of Things is one of the most widely used and advanced computer technologies today. This is due to the new generation of adoption, automation, reality-based intelligence that interconnects objects and infrastructure in everyday life. In this review paper, an attempt has been made to analyze IoT in detail, focusing on its transformative aspects in various aspects of IoT, particularly in sectors such as industry, automation, smart living, medicine, safety, and agriculture. IoT has wide acceptance, and various security aspects and scenarios have been introduced. Also, the heterogeneous nature of IoT's various sensor gadgets, their limited support aspects and scale of deployment create a well-sized, and vulnerable attack surface. We analyze key protection problems, inclusive of facts privateness breaches, unauthorized get admission to, denial-of-provider (DoS) assaults, and tool manipulation. Furthermore, we explore ability solutions and mitigation techniques, together with light-weight cryptography, sturdy authentication protocols, and the use of rising technologies like blockchain and machine mastering for enhanced chance detection. This paper concludes via emphasizing the vital need for a holistic protection technique that addresses vulnerabilities at each layer of the IoT structure to make certain a steady and reliable related future.***
Keywords: Internet of Things, Smart Applications of IoT, Security Issues, Possible Solutions.

I. INTRODUCTION

The Internet of Things is a powerful research topic in the current era of computer technology. It is a topic that can connect the physical world with the virtual world. In 1999, Kevin Ashton first coined the term Internet of Things, which he originally meant to refer to a network of physical objects equipped with sensor technology, software, and other modern technologies. This network technology system basically connects to other devices or systems via the internet and exchanges data. This ability enables higher levels of automation, real-time data collection, and smart decision-making, which goes beyond traditional human-computer interaction.

The applications that are the Internet of things has are quite varied and quite extensive. And as you can see, IoT can affect almost every part of modern life today. In today's daily life, this technology can provide a variety of smart benefits, in addition to additional energy efficiency. Example- Smart Lighting, Smart Home, Smart Security System, Monitoring. Also, the modernization of wearable devices in healthcare and patient monitoring from remote locations, and these systems can provide continuous data, As a result, doctors can treat patients by giving them the important feedback they need in time. The Internet of Things can also be used in agriculture. For example, it can provide information about soil temperature, moisture, or soil nutrient levels. Industrial IoT (IIoT), a part of IoT, is advancing Industry 4.0 by enabling predictive maintenance, optimizing supply chains, and automating factories, which increases productivity and lowers operational costs.

But as IoT continues to explode, it also brings a slew of security concerns. A number of IoT devices have low-end resources and are underpowered in terms of CPU and memory to accommodate heavyweight security protocols. Due to their ubiquitous and usually unprotected use, they are left open to attacks. Weaknesses are found at all stages of the stack, including the physical sensors down to cloud-based applications in which they serve as targets to many threats. Data security, of course, is a big concern because all kinds of sensitive information that's captured by devices whether it's health data from a smartwatch or location data from an automobile can be intercepted or stolen.

This paper aims to review modern IoT applications, carefully examining the security issues and weaknesses they bring. Efforts have also been made to find solutions to reduce these potential risks and create secure IoT Networks. Also, at the end of this paper, an attempt has been made to show some modern applications of smart Google authentication methods.

II. LITERATURE REVIEW

1) Review of "Internet of Things - An Overview" Author: Rupinderpal Kaur (April 2024) Kaur gives an overall concise and current review of the evolving technology that is known as the Internet of Things (IoT). IoT is presented as the technologies that have the most current value for research and are the main industry in comparison with AI and Robotics. Kaur demonstrates the ability to clearly illustrate how automated processes that interconnect devices to sensors can assist with human decision-making through automation and or data-based decision-making. In spite of this, the author does note that limited amounts of peer-reviewed academic research exist in this field; however, Kaur also provides an appropriate emphasis on the increasing significance of IoT in the present day to society. By discussing the above topics of connectivity, remote sensing, and intelligent device-to-device interactions, Kaur provides a broader understanding of these concepts to the reader, but Kaur only briefly touches upon the technical aspects of IoT, such as systems design, communications models, and protocols. Overall, this article is an easy-to-read and well-organized introduction to the field of IoT for readers who are new to the subject; Kaur's writing style is basic and coherent and places a great deal of importance on the significant effects that IoT will have on the future of society. This article is a very good reference for anyone who is interested in the emerging technologies industry.
2) A review internet of things (IoT) security challenges and issues (May 2023) Author(s): Dr. S. Thavamani, Ms. C. Nandhini, and Mr. T. Pradeep - The study by Thavamani, Nandhini, and Pradeep, discusses growth of the Internet of Things (IoT) and the security issues that come with it. The authors state that IoT is one of the most important technologies of this modern digital era and enables the interconnection of countless devices that provide a multitude of services and perform powerful data processing. The authors mention the countless number of IoT applications in healthcare, smart homes, industrial automation, and smart cities while also mentioning the many security issues that come with it. It is also stated that the rapid growth and advancement of the IoT, coupled with the rapid growth of devices that are smaller in size and greater in processing power provide a unique set of problems with respect to securing data, communications, and devices, retaining integrity. The authors also provide a number of security solutions and suggestions to reduce the most critical risks. Overall, this is a very informative and structured paper on the positive and negative aspects of IoT.
3) Internet of Things (IoT) Applications and Security Challenges (2023) Authors: Aswathy Suresh S. J. and Sreeshma Mohan. - Suresh and Mohan offer an in-depth analysis of the increasing scope of IoT application and the security challenges that come along with it in different sectors. The authors have emphasized that the increasing number of IoT devices in residential and industrial sectors is increasing the complexities of ensuring the security of these devices and systems. The paper clearly differentiates between IoT application in residential sectors, such as smart home devices (e.g., Amazon Echo and Google), and industrial sectors, such as IoT application in industries like manufacturing, oil and gas, pharmaceuticals, and water treatment. The authors have emphasized the security challenges faced by industries due to the increasing number of connected devices and data exchange between them. Each device and data exchange process is considered a potential target for cyber attacks. The most important part of the paper is the focus on cybersecurity in industrial sectors. The authors have emphasized the need for a multiple-layered security framework for ensuring the security of devices and data exchange. The authors have also emphasized the need for cooperation and coordination among different stakeholders in ensuring the security of IoT infrastructure. The paper provides a clear and understandable knowledge of the opportunities and security.
4) Review of "Communication Security Challenges of IoT" Author: Subhankar Sarkar (2023) Sarkar, dives right into the risks and security headaches that come with IoT communication systems. He starts by laying out what IoT actually is, then shows just how fast it's spreading into all sorts of tech fields. As these networks get bigger, Sarkar points out, the dangers grow too—think data getting snatched, privacy slipping away, or devices getting tampered with. He doesn't just skim the surface either. Sarkar calls out the big threats: people breaking in where they shouldn't, lazy encryption, and open channels where data can leak. He also talks about cloud integration and why locking that down matters. The paper isn't long, but Sarkar gets the point across: we need real solutions to keep these networks safe, and we need them now. His writing is straightforward and sticks to the real-world problems, making it easy for anyone new to IoT security to follow along. In the end, Sarkar's work actually moves the conversation forward. He spells out where we're vulnerable and basically says, "We have to do better." This paper lays a solid groundwork for anyone looking to dig deeper and build stronger, safer IoT systems.
5) Review of "A Review on Internet of Things" Authors: Aditi Rajesh Nimodiya and Shruti Sunil Ajankar (2022) - Nimodiya and Ajankar in their paper give a picture of the Internet of Things. They show how it connects devices in the digital worlds. The authors explain the parts, structure and features of IoT and its many uses. This helps readers understand IoT clearly. great part of the paper is how it talks about how communication models have changed. They go from people talking to machines to machines talking to each other. This shows how big a role IoT plays in how we connect today. The authors also look at the bad

sides of IoT. They see its potential but also its problems. The paper mainly just describes IoT. Does not deeply analyze new IoT technologies. So it is a starting point for readers and researchers. In Nimodiya and Ajankars paper is a helpful and fair review of IoT. It covers the ideas real-life uses and social effects of the Internet of Things. It is a guide for people who want to know about IoTs growth and how it affects daily life. Nimodiya and Ajankars work on IoT is very informative. Their paper, on Internet of Things helps us understand its impact. The Internet of Things has applications. Nimodiya and Ajankar discuss IoT in detail.

6) "A Review Paper of Security in Internet of Things (IoT) (2021)" Authors: Nagesh U. B., Nayana M. S., Shruthi C. S., Sudeep Poojary, Vaishnavi P. S., and Vshker Mayengbam. - In the IoT security sphere, all authors provide an in-depth overview of the state of the art. The authors describe the impact of IoT on everyday life with billions of devices used in smart healthcare, smart transport, and smart infrastructure. The review's central theme is the new security vulnerabilities created by the intercommunication of devices and the large-scale exchange of data. It suggests an IoT security attack taxonomy by purpose and explains how the threats affect data privacy and the integrity of the networks. The authors review security measures, classify them based on areas of application, and map out existing frameworks. The paper is relevant because of its research gaps and challenges. The addition of research directions and challenges elevates the paper. The review is strong, but a more thorough examination of the technical details, which include cryptography and authentication, would lead to a more balanced representation of IoT security. The review is clear, systematic, and primarily focused on data protection for researchers focused on IoT cybersecurity.

7) A Review Paper on Internet of Things (IoT) and Its Applications (2020) Authors: Mrs. Sarika A. Korade, Dr. Vinit Kotak, and Mrs. Asha Durafe. In their paper, Korade, Kotak, and Durafe systematically present the Internet of Things (IoT) and the fundamentals of its function, as well as its applications in several fields. They highlight the significance of IoT as a breakthrough technology in enabling M2M (machine-to-machine) communication via the use of sensors, actuors, and the intelligent exchange of information. The authors present all the important components of the IoT, such as IoT architecture, edge computing, the field-cloud model and protocols, and the application of IoT in smart cities, smart grids, smart healthcare, and smart agriculture. The authors describe the functional flow of IoT systems and explain the importance of IoT in improving operational and managerial efficiency, automation, and making informed decisions. They also consider the merits and demerits of IoT, as well as the implications of privacy and data management. Although the paper does a good job at articulating the concept of the IoT, it lacks coverage of the relevant empirical or technical aspects. Still, it sufficiently introduces the subject of IoT for the benefit of readers and students. The paper is concise, yet it comprehensively covers relevant and important topics, making it clear, and easy to use for the study of how IoT technologies integrate and support the digital infrastructure and applications of the IoT in the real world.

8) Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios (2019) Authors: Kinza Shafique, Sameer Qazi, Bilal A. Khawaja, Farah Sabir, and Muhammad Mustaqim. - Shafique et al. provide a comprehensive examination of the merger of the Internet of Things (IoT) with Fifth Generation (5G) communications systems, including the analysis of existing problems and the review of the new trends. The paper discusses the transformations in connection and service provision brought about by high data rates, low latency, and high capacity of bandwidth. A remarkable feature of this paper is the presentation of MIMO, Network Function Virtualization (NFV), Software Defined Wireless Sensor Networks (SD-WSN), and cognitive radio as enabling technologies. The authors provide a vision on the development of heterogeneous networks (HetNets) and their contribution towards seamless IoT connection. The paper also notes the problems of maintaining Quality of Service (QoS), of ensuring the ecosystem 5G-IoT is scalable, and of the data security. The study successfully demonstrates the contribution of artificial intelligence and machine learning towards improvement of the next generation of smart systems. The paper presents an advanced technological study and broad survey that illustrates the impact of IoT and 5G technologies convergence on the development of digital ecosystems and technological advancement.

9) Review of "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures" by Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar (2019) Hassija et al. provide a thorough and highly technical review of the security issues of the Internet of Things. The authors review the different IoT applications and provide a comprehensive list of the respective security threats and design vulnerabilities. A major contribution of this lesson is the detailed evaluation of the emerging technologies namely, Blockchain, Fog Computing, Edge Computing, and Machine Learning as the main facilitators of IoT security and the innovative ways they can improve the various techniques employed to secure authentication, privacy, and data integrity of interconnected systems. The authors note the importance of developing IoT

systems that are secure, scalable, and adaptive to changes in the cyber threat environment. The authors provide a much-required combination of theory and practical approaches in a way that is useful to researchers and those in the industry, and most importantly, to practitioners. This lesson is of high value to the body of knowledge on Internet of Things. It, most importantly, demonstrates the need to strike a balance between the ways in which internet-connected devices can communicate and offer a high level of security, and for this reason, it provides a solid platform for other researchers to start on for lessons on secure Internet of Things and trust-based architecture.

10) Internet of Things (IoT) Applications and Security Challenges: A Review (2019) Authors: Mohit Kumar Saini and Rakesh Kumar Saini - The paper by Saini and Saini (2019) is an informative paper that discusses the development of Internet of Things (IoT) and the security challenges that are associated with it. The paper is a good example of how IoT has revolutionized global communication by ensuring that people and intelligent systems are connected. The authors have particularly focused on the development of IoT in two major sectors: the use of IoT in homes and the use of IoT in industries. The authors have discussed these concepts very well and have shown how the use of smart devices in homes and industries has led to an increased need for cybersecurity. The authors have also cited examples of how IoT is being used by Amazon Echo and have shown how IoT is being used in industries such as manufacturing, oil and gas, and pharmaceuticals. The authors have also shown how cybersecurity is important in these industries and how any disruption in these industries may lead to economic losses. The authors have also shown the complexities of ensuring the security of IoT systems and have particularly shown how data transmission is a major concern in ensuring the security of IoT systems.

11) Internet of Things (IoT): Research Challenges and Future Applications (2019) Author: Abdel Rahman H. Hussein. - Hussein wrote a paper about the Internet of Things. He talked about how it can be used in areas and the problems that still need to be solved. The paper looks at how the Internet of Things can be used in cities, healthcare, agriculture, logistics and smart environments. The Internet of Things is expected to change parts of our lives. Hussein said that even though Internet of Things technologies have come a way there are still issues with how different systems work together handling large amounts of data and keeping information safe and private. A good thing about this paper is that it covers a lot of ground linking technology development with real-world use. The author thinks the Internet of Things is a field that involves information technology, computer science and engineering and that it has a lot of research potential. The paper also looks at directions for Internet of Things innovation suggesting more studies on smart systems and adaptive architectures. Even though the paper does not include data or examples it provides a lot of thought and a forward-looking view making it a valuable contribution. Overall Hussein's paper is a discussion of the Internet of Things research landscape. It balances excitement, for its potential to change things with an awareness of the technical and ethical challenges it poses. The Internet of Things has a lot of potential. It also has many challenges.

III. INTERNET OF THINGS (IOT)

The Internet of Things, or what we call IoT for short, refers to a global network of infrastructure that connects embedded technological objects such as sensors, processors, and actuators. This technology can collect and process information from the surrounding environment. That is, it can communicate with all internet-based electronic devices and systems via the internet. Internet of Things aspires to bridge the physical and the digital worlds for automation, analytics, and other services. Designed IoT systems are generally structured with multiple layers, which can include: the Perception Layer, which has the devices that physically sense the environment; the Network Layer, which transmits the data; the Middleware Layer, which processes and manages data; and the Application Layer, which interfaces with the user. Such layering improves modularity but also mandates standardization to facilitate interoperability and security, as layers add complexity.

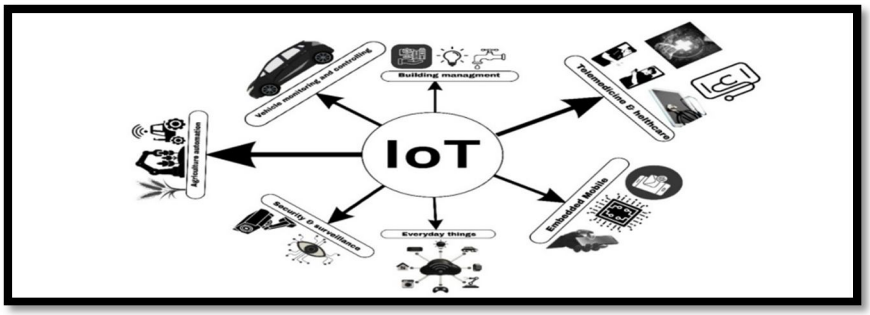


Figure-1. Internet of Things and Applications.

IV. SMART AND MODERN APPLICATIONS OF IOT

The growth of IoT has led to many smart and modern applications that are changing industries and everyday life. These applications use connected devices to gather, process, and respond to data in real time. This creates more efficiency and new user experiences. Some of the modern Internet of Things applications are Described below-

1) Smart Homes and Buildings: IoT makes our homes and workplaces smart and automated. Smart homes rely on internet-connected devices such as smart light bulbs, connected thermostats (Nest), and security cameras (Ring) to enable convenience, energy savings, and bolstered security. A smart thermostat, for instance, is capable of learning the user's schedule and making temperature adjustments as necessary to help save energy. In the corporate sector, for example, IoT sensors can track building occupancy and allow HVAC systems and lighting to be adjusted according to demand, resulting in potentially large cost savings. Fire and flood detection systems based on IoT could be used to give early warnings for the safety of the inhabitants.
2) Healthcare (IoMT): Improving patient care and remote monitoring outcomes have been greatly improved with the Internet of Medical Things (IoMT). Wearable devices such as smartwatches and fitness trackers can monitor things like heart rate and sleep patterns. For patients suffering from chronic illnesses, IoT devices like smart pill dispensers and continuous glucose monitors can interact with healthcare professionals, providing them with necessary data and alleviating the healthcare system of unnecessary hospital visits. In a hospital scenario, smart medical devices can collect and transmit invaluable patient data in real-time. Care can be adapted and streamlined, creating a positive impact on patient outcomes. The Internet of Medical Things is also great for the elderly as it allows them to live independently for longer and tracks their health continuously.
3) Smart Agriculture (Agri-Tech): The Internet of Things (IoT) is bringing about a revolutionary transformation in the agricultural sector by enabling precision farming. Sensors deployed in the fields collect data regarding soil moisture, temperature, and nutrient levels. Subsequently, by analyzing this data, it becomes possible to generate highly effective and actionable insights for farmers, assisting them in optimizing irrigation schedules, ensuring the efficient application of fertilizers and pesticides, and forecasting crop yields. IoT sensor-equipped drones are capable of surveying vast tracts of farmland to monitor crop health and detect harmful pests. This technology not only enhances crop productivity but also minimizes the consumption of resources such as water and pesticides, thereby making a significant contribution toward maintaining ecological balance.
4) Industrial IoT (IIoT): The Internet of Things (IoT) has made a significant impact on the industrial sector, driving the Industry 4.0 revolution. It connects sensors and control systems to a network, enabling real-time monitoring and automation. Predictive maintenance is a key application of IoT, wherein equipment sensors detect signs of wear and tear, allowing for the scheduling of maintenance before any faults actually occur. This prevents costly production downtime and extends the lifespan of machinery. IoT also enhances supply chain management by tracking goods during transit and providing real-time data on their location and condition. This transparency optimizes logistics, minimizes losses, and ensures product quality.
5) Smart Cities and Transportation: The 'Internet of Things' (IoT) serves as the fundamental cornerstone of smart cities, where it is utilized for the management and development of urban infrastructure. Smart streetlights can automatically adjust their brightness based on the presence of pedestrians, thereby conserving energy. IoT-enabled waste management systems can alert sanitation departments when waste bins are full, making waste collection routes more streamlined and efficient. IoT sensors embedded in roads and vehicles can monitor traffic flow and speed, provide real-time data on congestion, and facilitate autonomous driving systems. Smart parking systems guide drivers to available parking spaces, which helps alleviate traffic congestion. Such applications enhance the overall efficiency and sustainability of the city while improving the quality of life for its residents.
6) IoT Used in Disaster Preparedness: Currently, the Internet of Things is used in various fields and also plays an important role in Disaster Preparedness Recovery and Response. By using a network of connected devices, authorities can get real-time information about environmental conditions and infrastructure status. This helps them make informed decisions that save lives and reduce damage. If we use IoT related sensor technologies to monitor potential threats in disaster management, the task of dealing with disasters can be made easier. For example, Smart river water level monitoring and warning for flood control. In the case of earthquakes, monitoring of subsurface waves or smart investigation of the cause of earthquakes and providing warnings on multiple issues. Also, atmospheric pressure, wind speed monitoring, and rapid population migration, etc. In the response phase, we use Internet of Things devices - helping to coordinate urgent tasks more effectively. For example, damaged areas can be surveyed by drones with thermal sensors or other sensors through high-resolution cameras or smart drones can be deployed to rescue or identify people trapped in remote areas, or to assess the extent of damage. Where rescue teams cannot easily enter. Another way, wearable IoT devices on first responders can monitor their vital signs and location. This ensures their safety and improves team coordination. It can also be used to remotely monitor traffic lights, manage smart infrastructure in places like

grids, and deliver medicines to patients in hospitals. In terms of recovery, IoT helps with long-term monitoring and reconstruction. In particular, it helps in assessing the infrastructure of a place or object after a disaster.

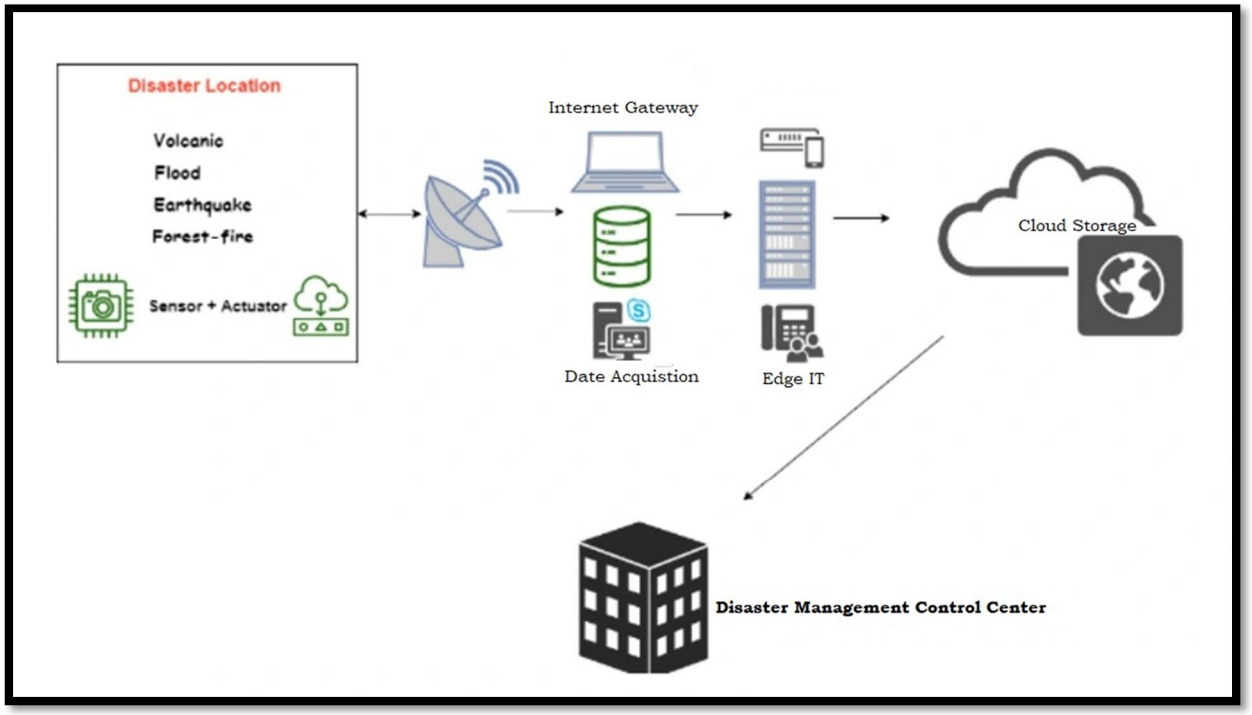


Figure-2. IoT In Disaster Management.

V. SECURITY ISSUES OF INTERNET OF THINGS

IoT is exceptionally diverse with its breadth, which results in unique security challenges that differ from traditional IT systems. This is due to the number of devices as well as their resource limitations. In addition, the systems are set in a distributed architecture which can make them very appealing candidates for a cyberattack.

1) Weak Authentication and Authorization: Most IoT devices come with weak, default passwords or without any passwords at all. Attackers find it simple to target these devices and use automated scripts to look for and take advantage of such vulnerabilities. If compromised, the attacker can gain access to the whole network or use in a botnet; this is made possible by just compromising one device. There is no standard, strong authentication method for different types of devices from very basic sensors up to complex industrial controllers that would be considered a critical gap in security.

2) Insecure Communication Protocols: The communication between the IoT devices and the cloud, or with one another, frequently is not encrypted at all or only supports weak protocols. Capture data, including personal data and financial information; Interfere with the server's operational logic2, proxy1. preprocessing(direct communication between plants needs to be rerouted through a third party server that could b2 e manipulated) Attackers can act as man-in-the-middle attackers for unauthorized handling or even injection of malicious commands. Although some devices implement encryption, they may do it wrong or use weak algorithms, and thus can be attacked cryptographically. Low-power computers in many devices restrict the use of advanced and relatively difficult encryption, which exacerbates this problem.

3) Firmware and Software Vulnerabilities: There's a lot of IoT devices out there which are using lightweight or home-brew operating systems created without security best practices. This results in a lot of vulnerabilities, like buffer overflows and injections. Also, a large number of existing IoT devices are also not designed with an over-the-air (OTA) firmware update facility and are therefore unable to be patched from known security vulnerabilities. Hackers can use these unfixed vulnerabilities to take full control of a device, install malware, or jump to another corner of the network.

4) Data Privacy Concerns: Connected objects collect an extremely large and often intimate amount of data. Smartwatches record health data, smart speakers listen to conversations, and security cameras film video. This data can be easily hacked and thus privacy breaches will emerge. Insufficient data governance and data residing in multiple places (e.g., on the device, at the edge, in cloud) further complicates consistent privacy protection.

5) Denial-of-Service (DoS) and Botnet Attacks: The most frequently reported security problem is the leveraging of vulnerable IoT devices for massive distributed denial-of-service (DDoS) attacks. Botnets such as the Mirai botnet, which infect thousands or millions of vulnerable devices, are capable of harnessing the combined power of all those infected machines to flood a target's network and knock out internet services. These attacks are extremely difficult to protect against because they originate from a large number of seemingly unrelated IP addresses around the planet, which would be nearly impossible to block.

VI. POSSIBLE SECURITY SOLUTIONS FOR IOT

The specific challenges surrounding the security of IoT devices requires an encompassing and strategic approach that takes into consideration the entire system's life cycle, from the moment the devices are developed to the point where the devices' data are fully processed.

1) Strong Authentication and Access Control: Implementing strong authentication mechanisms is the first and most important step. This means getting rid of default credentials and requiring strong and use unique passwords for each device. Multi-factor authentication (MFA) should be a standard feature for devices that manage sensitive data or control critical systems. Access control policies must be in place to ensure that only authorized users and devices can access specific resources, following the principle of least privilege. For machine-to-machine (M2M) communication, using certificate-based authentication and secure key management is vital to stop unauthorized device impersonation.

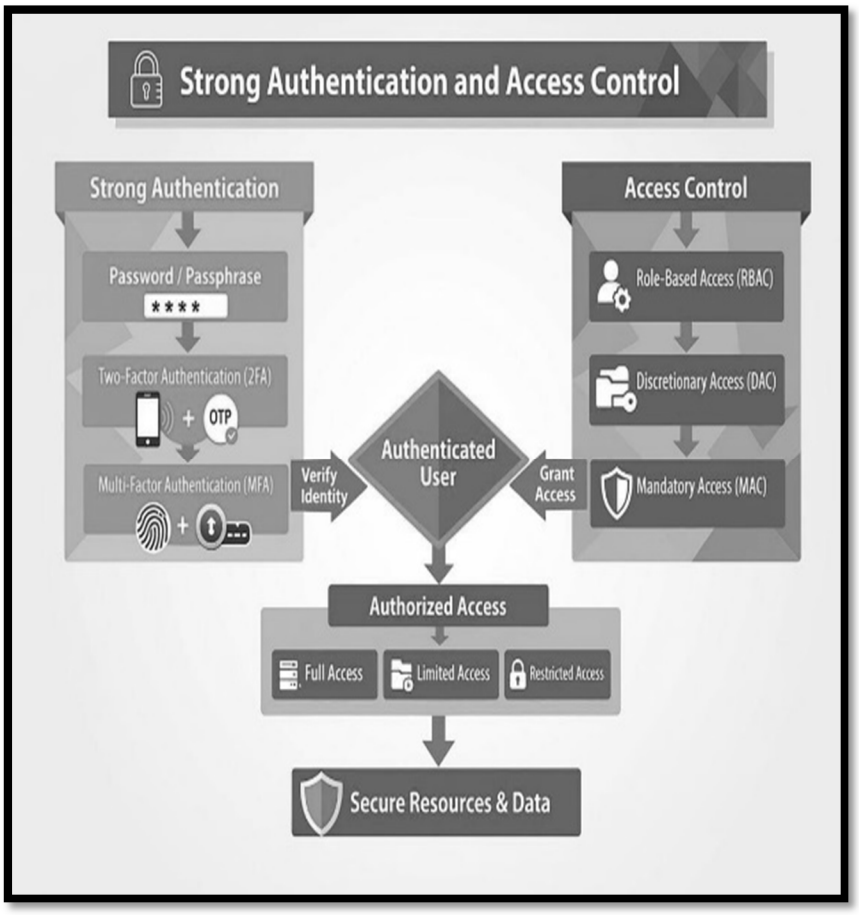


Figure 3 - Strong Authentication and Access Control Process.

2) Secure Communication and Data Encryption: You should Encrypt everything in motion as well at rest data to secure it from sniffing and unauthorized access. Lightweight cryptographic algorithms like the one proposed by IEEE 802.15.4 security framework are specifically defined for resource-constrained devices, and their design allows these devices to encrypt/decrypt without causing a significant energy waste. Protection of data exchanges transmitted over the network requires use of confidentiality and/or integrity algorithms, but not all security protocols provide both.

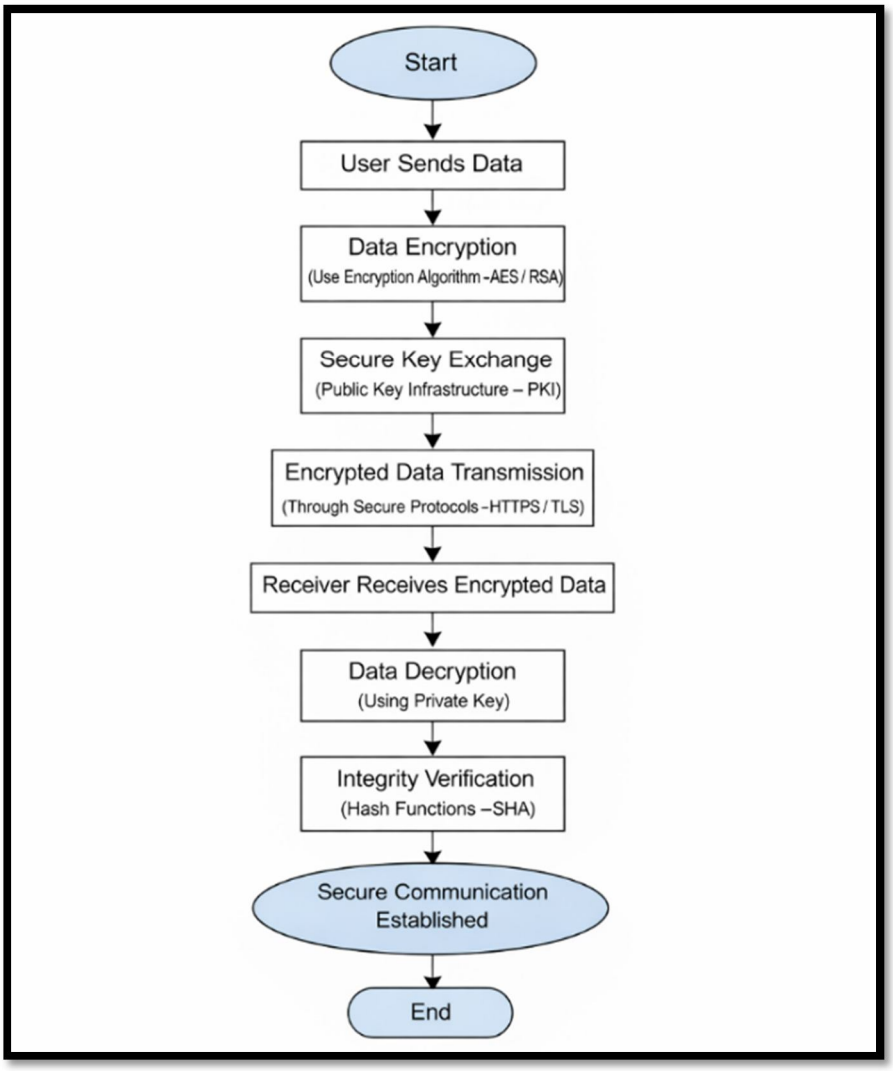


Figure 4 – Algorithm of Secure Communication and Data Encryption.

3) Regular Firmware Updates and Patching: An overall secure and trustworthy firmware update OTA have to be a mandatory function for all of the IoT devices in order to prevent firmware vulnerabilities. Support from the manufacturers and regular security updates must be guaranteed. Secure booting means a device loads only firmware that is authentic -- or hasn't been tampered with to call some shady behaviour upon itself. Implementing a secure SDLC which incorporates threat modelling and security testing from the design stage is key as well.

4) Network Segmentation and Intrusion Detection: Network segmentation can limit the impact of any compromised device. If the IoT devices run on a separate, isolated segment for the network, it will not be easy for the attacker to perform lateral movement inside other important places in networks like corporate servers or personal computers simply by compromising one device. IDS/IPS tuned to rules fit IoT traffic patterns that can spot and dynamically block much malicious activity - even this level of port scanning and unauthorized data exfiltration.

5) Blockchain and Distributed Ledger Technologies (DLT): Blockchain has recently been considered the best solution for IoT security, especially in matters of trust and integrity. Decentralized and immutable facts can be used to prove ultimate records of device identities and data. For example, it is possible to create a secure method for registering new IoT devices so that only legitimate devices are allowed to join the network. It may also be used in creating an auditable log recording all transactions on data, thus assuring data integrity and provenance itself. Although blockchain will result in computational overhead, its characteristics define it as a very applicable mechanism for instilling trust and ensuring security within a decentralized IoT environment.

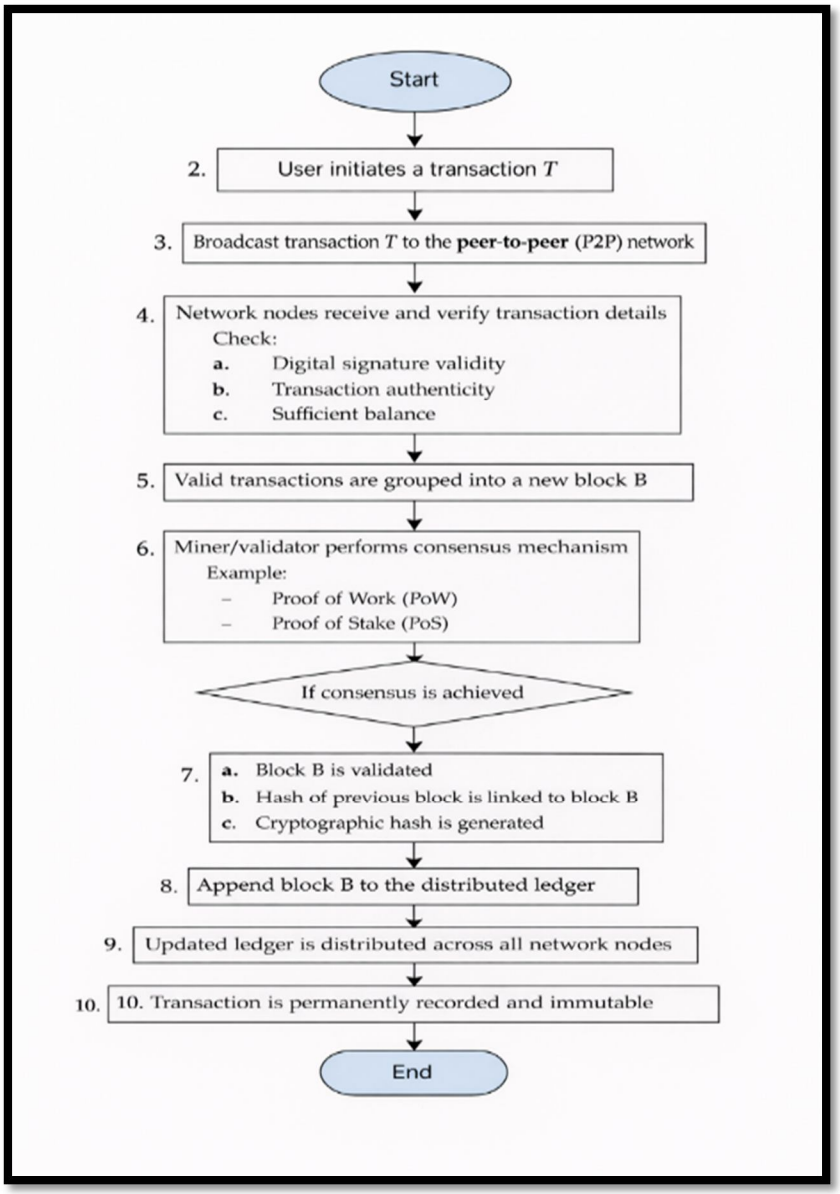


Figure 5 – Algorithm of Blockchain and Distributed Ledger Technologies (DLT).

VII. PROPOSED MODEL

At the end of this paper, we have shown the aspects of common authentication methods to easily ensure the security of IoT Devices or IoT applications through a smart application.

1) Role of Google Authenticator in IoT Security: Multi-Factor Authentication (MFA) is an important part of protecting Internet of Things (IoT) networks. Google Authenticator is one of the MFA solutions that many organizations use and provides another layer of security by using Time-based One-Time Passwords (TOTP) as defined by RFC 6238. TOTP is used in IoT environments to help ensure that users' authentication to devices, cloud services and management dashboards is secure. TOTP also adds another benefit of making access credentials (like username and password) short-lived. This helps to minimize the risk of credential theft and replay attacks. Google Authenticator is used when a user logs in to an IoT management console or when a user is pairing a new device to their account. By supporting MFA using standard cryptographic protocols, Google Authenticator helps to strengthen the security of IoT systems and increase the security and trust that users will have in those systems as they use them in networks containing multiple distributed devices.

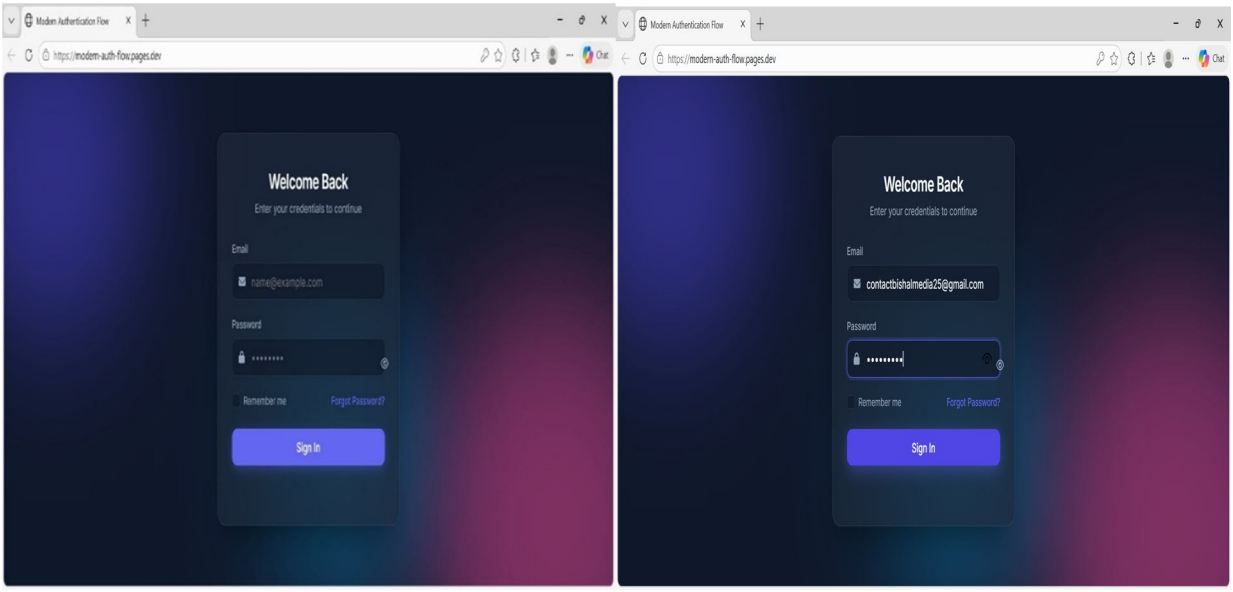


Figure 6 (I & II) – Login Page. (Proposed Model).

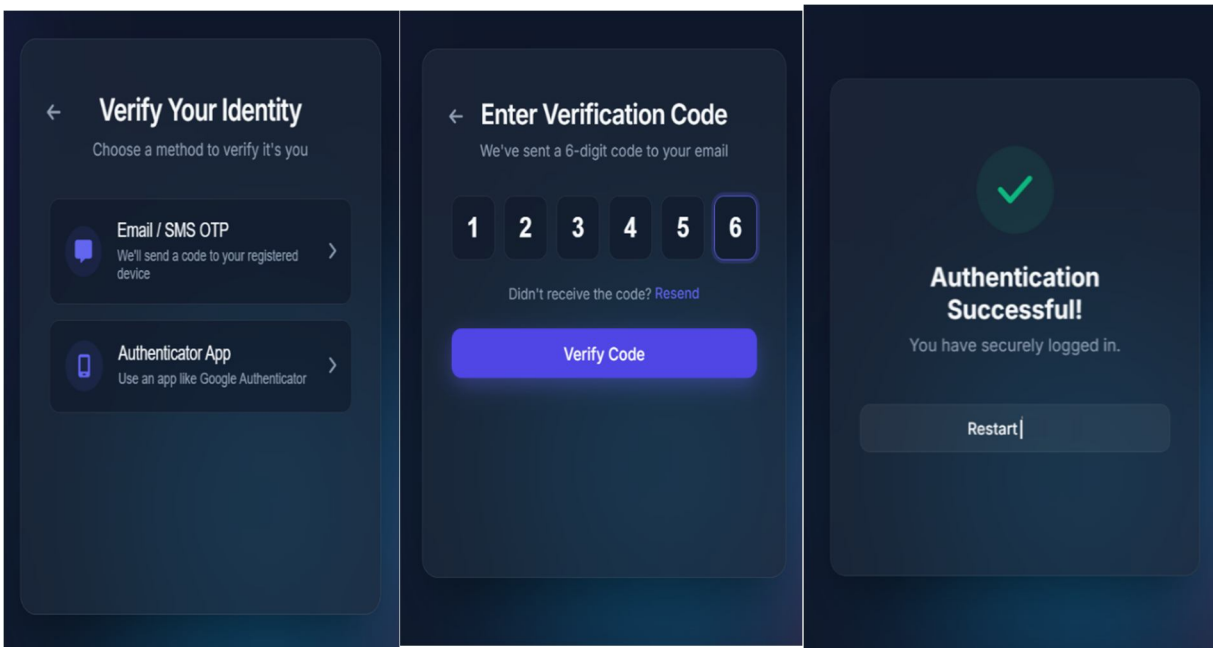


Figure 7 (I & II & III) – Verify Identity Page Enter Authentication Code receved through Email or SMS and Verify this Code.

In above *(Figure 6)* this experimental application, to access IoT Devices, the User must first go throughan email or SMS Verification process.

As a second example, *(Figure 7)* we have shown a modern implementation of the Google authentication method: Where to access any Internet of Things platform, the user first has to scan the QR Code and then complete the smart authentication process through the 6-digit password received.And the user gets permission to enter the main part for work. This QR Code method is more modern than the OTP module and can be changed at a specific time, so the security system can work very well in this process.

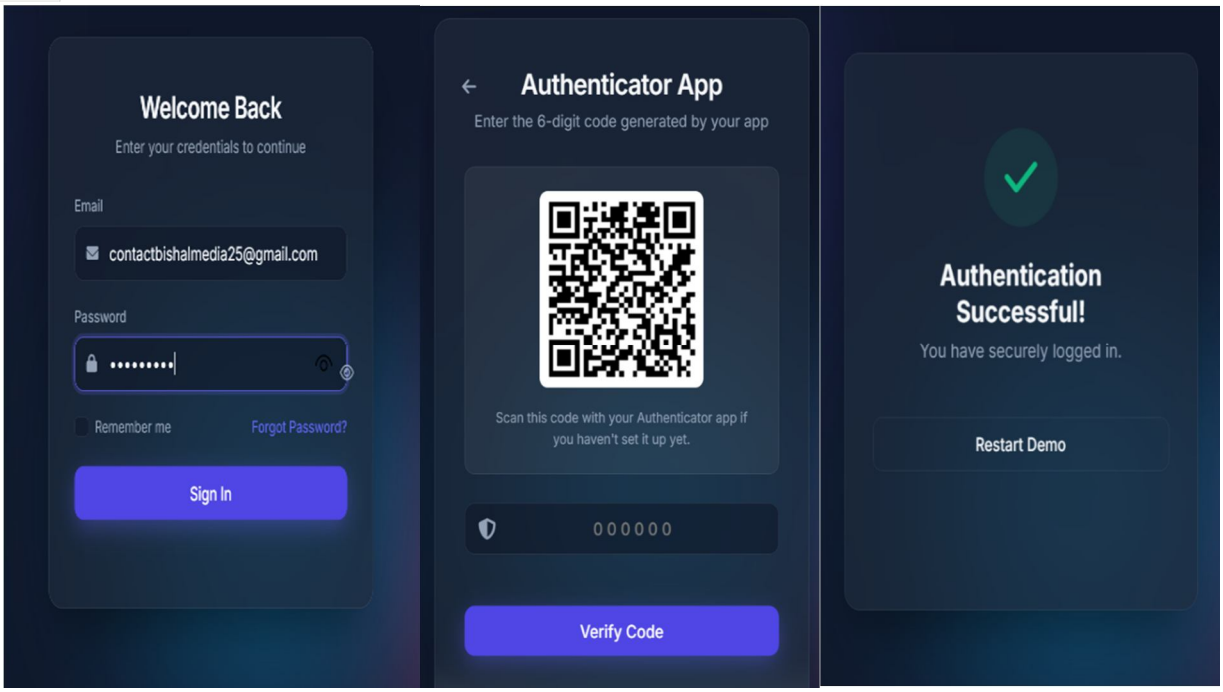


Figure 7 (I & II & III) - Login Page, Google Authenticator Verification Page and Authentication Process.

That is, here an application is shown that the user logs in first. And the main IoT system can be easily accessed through scanning using the Google Authenticator app with the new password. As a result, the security of the core IoT platform remains secure.

VIII. CONCLUSION

The Internet of Things is a significant technological advancement. IoT integrates devices with digital systems, and, due to this integration, it makes the automation of systems easier and gives efficiencies and insights based on data. IoT can change and improve industries such as smart homes, healthcare, industrial automation, and smart cities. However, the IoT still has some challenges. Primarily, there remain some major security and privacy issues: weak authentication, insecure communication, and unpatched software vulnerabilities provide and has already been exploited a very weak and wide attack surface that has already been exploited in large-scale cyber-attacks. A proactive and multi-layered approach to security will help mitigate challenges to realizing the true potential of the connected world. Strong security protocols include robust authentication, end-to-end data encryption, and regular firmware updates. Throughout the research paper, we have highlighted the Internet of Things and its practical aspects, as well as reviewed several previous papers. In this paper security risks of Internet of Things ere also discussed. Finally, we have tried to give an idea of the Smart modern application of the Google authentication system at the end of this research paper. A security-first design with ongoing adaptation to new threats will create an IoT ecosystem with the trust and resilience to enhance our lives and society.

REFERENCES

[1] IEEE Standards Association. (n.d.). IEEE P2413: Standard for an Architectural Framework for the Internet of Things (IoT). Retrieved from standards.ieee.org.
[2] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660.
[3] Sicari, S., Rizzardi, A., Grieco, G. M., & Coen-Porisini, A. (2015). Security, privacy, and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–162.
[4] Roman, R., Al-Rodhan, J., & Lopez, J. (2011). A survey of cryptographic primitives and security protocols for the Internet of Things. Journal of Sensor and Actuator Networks, 1(2), 291–311.
[5] Hasan, M. M., & Khan, M. N. (2018). Securing the Internet of Things: A survey. Journal of Network and Computer Applications, 103, 110–123.
[6] Khan, M. A., & Salah, K. (2018). IoT security: Review, challenges, and solutions. Future Generation Computer Systems, 82, 395–411.
[7] Conti, M., & Lal, C. (2019). Blockchain for securing the Internet of Things. IEEE Access, 7, 102573-102588.
[8] Sisinni, E., Saifullah, A., Han, J., Jantunen, H., & Ghavami, M. (2018). Industrial Internet of Things: A survey on architectural aspects, security issues, and future directions. IEEE Transactions on Industrial Informatics, 14(11), 5285–5296.
[9] Sarkar, Subhankar., (2025). Smart-Review on Disaster and its Prevention Management in India. International Journal of Advanced Research in Science Communication and Technology, 26–56. https://doi.org/10.48175/ijarsct-23705

[10] Dhinakaran, D., Udhaya Sankar, S. M., Latha, B. C., Anns, A. E. J., & Sri, V. K. (2023). "Dam Management and Disaster Monitoring System using IoT." 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), 1197–1201. (A specific application of IoT in dam management for flood prevention.
[11] Sarkar, Subhankar. "Communication Security Challenges of IoT." International Journal of Novel Research and Development (IJNRD) 8, no. 9 (2023). d43-d51. https://www.ijnrd.org/papers/IJNRD2309306.pdf
[12] Fraser, H. (2025, July 11). What is an IoT Security Solution - Asimily. Asimily. https://asimily.com/blog/iot-security-solutions-and-how-they-protect-connected-devices/
[13] Spektor, H. (2024, July 28). IoT security solutions: key features and 8 solutions you should know. Sternum IoT. https://sternumiot.com/iot-blog/iot-security-solutions-key-features-and-8-solutions-you-should-know/
[14] What is IoT Security? Definition and Challenges of IoT Security | Fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/iot-security
[15] Prolim. (2025, December 16). Security architecture in IoT - PROLIM. PROLIM. https://www.prolim.com/iot/security-architecture-in-iot/
[16] National Institute of Standards and Technology (2017). Digital Identity Guidelines (NIST Special Publication 800-63). Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.SP.800-63
[17] Melanie Swan (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.
[18] Sarkar, S., & Roychowdhury, S. (2023). Authentication authorization and security issues in cloud computing. International Journal for Research in Applied Science and Engineering Technology, 11(11), 1275–1283. https://doi.org/10.22214/ijraset.2023.56670
[19] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, & Steven Goldfeder (2016).
[20] Olshtein, A. (2026, March 23). Google Cloud Authenticator: The Hidden Mechanisms of Passwordless Authentication. Unit 42. https://unit42.paloaltonetworks.com/passwordless-authentication/
[21] Abdalzaher, M., Krichen, M., Yiltas-Kaplan, D., Ben Dhaou, I., & Adoni, W. (2023). Early Detection of Earthquakes Using IoT and Cloud Infrastructure: A Survey. Sustainability, 15(15), 11713. https://doi.org/10.3390/su151511713
[22] Addressing security risks in IoT by safeguarding privacy and networks of connected devices. (2024, November 12). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/10867375

Author Details

Mr. Bishal Biswas. Corresponding Author

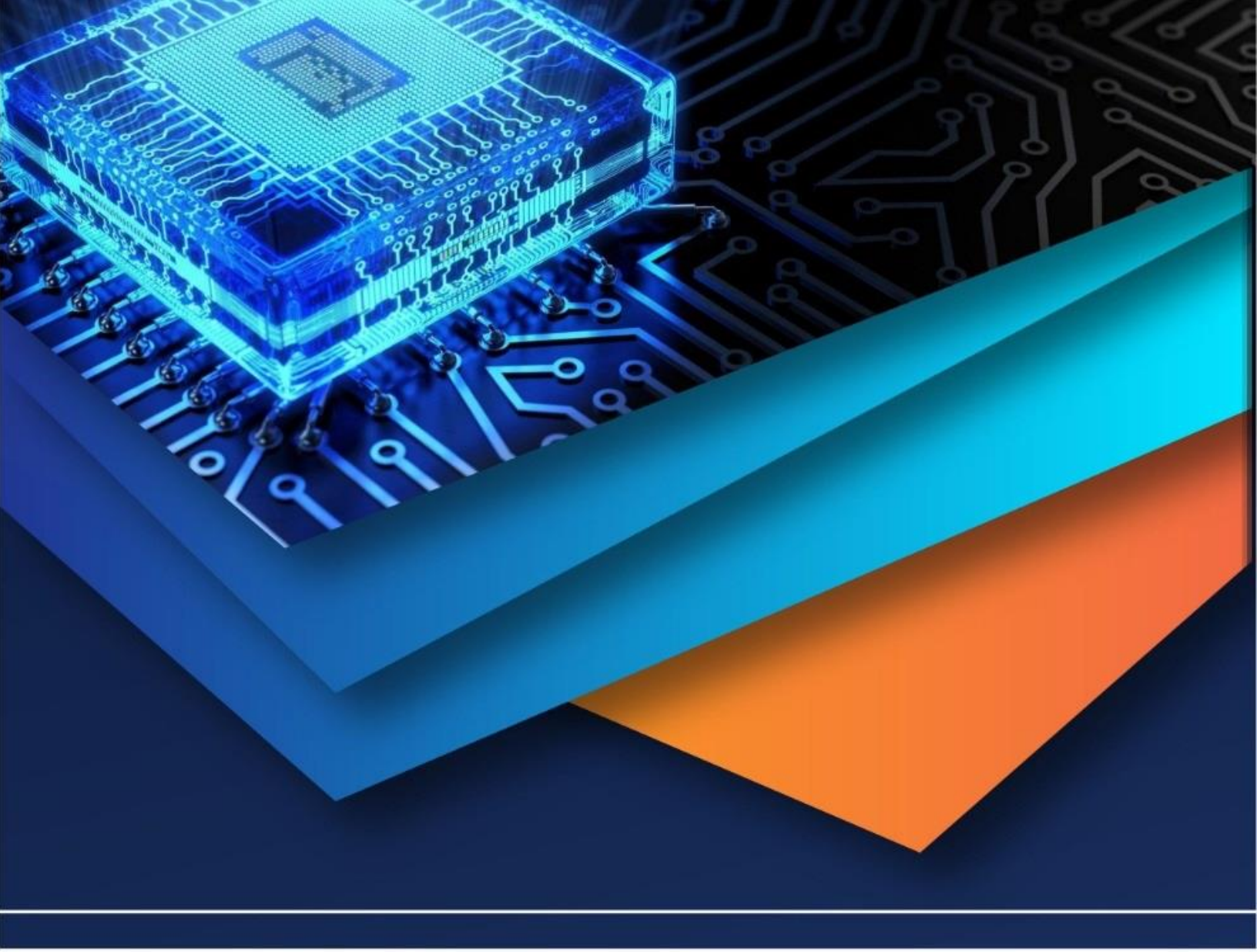
B.Tech-CSE, M.Tech – CSE. Pursing* from
Bengal Institute of Technology and Management. (BITM).
Santiniketan, Birbhum, West Bengal. India.
Research Interest- Internet of Things, Machin Learning, Network Security.
Email- contactbishalmedia25@gmail.com

Mr. Subhankar Sarkar

Co-Author
Ph.D. Enrolled - Department of Computer Science and Engineering. –
Maulana Abul Kalam Azad University of Technology, (Formerly Known As W.B.U.T.).
Simhat, Haringhata, Nadia, West Bengal. India.
Research Interest- Internet of Things, Machin Learning, Mathematical Modelling, Disaster Management.
Email- elinksuvankar.sarkar@gmail.com

Mr. Soumen Bhowmik

Co-Author
Assistant Professor & HOD - Department of CSE, Bengal Institute of Technology and Management. (BITM). Santiniketan, Birbhum, West Bengal. India.
Email- Bhowmik.soumen.cse@gmail.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY