Enhancing Safety Measures in IoT with 5G-Enabled Networks: A Case Study

Prithviraj Singh SOLANKI

Assistant Professor, Computer Engineering, Hansaba College of Engineering & Technology, Gokul Global University, Siddhpur
prithvisingh2488@gmail.com

Abstract - 5G technology plays a pivotal role in enabling the integration of diverse IoT devices, which are projected to reach 31 billion by 2020 and 74 billion by 2025. However, this exponential growth also amplifies the potential for cyber attacks as these interconnected devices communicate and share data on the cloud. To address this concern, the establishment of a robust and secure architecture becomes crucial for heterogeneous devices within 5G-based IoT environments.While IoT devices leverage 5G networks for seamless communication, the vast amount of data processed in cloud-based services becomes vulnerable to potential breaches in 5G communication systems. Adversaries can exploit various attack vectors, including unauthorized access to IoT devices and applications, such as DoS attacks, malware, masquerading, eavesdropping, physical attacks, botnets, spoofing, and other potential threats [3]. Protecting IoT-based devices necessitates more than just relying on traditional security measures like stream cipher algorithms, hash functions, AES, DES, RSA, ECC, SHA, and pseudorandom number generators. In order to enhance the security of IoT devices, there is a growing need to explore innovative techniques like blockchain and leverage the new concepts of the Golden Prime Ratio. Integrating these advanced cryptographic concepts can provide heightened security across software applications, hardware sensors, firmware, configuration files, security policies, network activities, device identification, IP address tracing, user behavior, and file system protection [1]. By embracing these techniques, IoT devices can mitigate potential vulnerabilities and reinforce their resilience against cyber threats.

Keywords - *IoT, Security, Cryptography, Golden Prime Ration, 5G.*

DOI: 10.48047/ecb/2023.12.1.579

I. INTRODUCTION

The convergence of IoT devices with the 5G network introduces security challenges, including the risk of packet sniffing and unauthorized code injection, which can manipulate the services of the IoT-based 5G network. As the future unfolds, the 5G network will exhibit scalability, versatility, and energy efficiency, making it ideal for supporting a hyper-connected ecosystem of IoT devices. The integration of 5G in IoT ecosystems will be characterized by low latency, high bandwidth, increased system capacity, high connection density, mobility, and a multi-tenancy service architecture. This opens up possibilities for deploying a multitude of devices across various applications such as smart cities, businesses, homes, cars, healthcare, and farming. However, ensuring the security of internet-connected objects without human intervention presents a critical challenge. Security and privacy concerns rise to a higher level due to the inherent risks associated with connecting numerous IoT devices and transmitting large volumes of big data over the cloud through 5G [10]. The concept of smart "things" or "objects" represents digitally or virtually self-functioning entities, and the focus of IoT is to create an intelligent environment by leveraging technologies such as nanoelectronics, 5G communications, diverse sensors, smart handsets, embedded systems, and cloud services. To fully harness the benefits of IoT for society, robust security measures must be implemented to safeguard IoT devices within the dynamic landscape of a 5G-enabled network [9]. The integration of 5G technologies with the Internet of Things (IoT) opens up new avenues for connectivity and innovation. However, this convergence also brings forth unique security challenges that must be addressed to ensure the safety and integrity of IoT devices and the data they handle. This research paper delves into the implementation of robust safety measures in IoT environments powered by 5G networks. By conducting a thorough analysis of essential aspects such as authentication mechanisms, encrypted communication protocols, secure firmware updates, access controls, intrusion detection systems, physical security measures, and regular security audits, this study aims to provide practical insights into effectively securing IoT devices within the realm of 5G. To illustrate the practical application of these safety measures, a compelling case study is presented, highlighting their effectiveness in a real-world scenario [8].

II. APPLICATION AREAS OF IOT

The Internet of Things (IoT) revolutionizes the connectivity of everyday objects, which are embedded with electronics, software, and sensors, allowing them to collect and exchange data over the internet and through cloud-based systems. IoT provides a platform that facilitates the interconnection of various entities worldwide, enabling interaction, collaboration, and a reduced dependence on human intervention. It stands as one of the most significant technologies shaping our world today. Within the IoT ecosystem, heterogeneous devices connect to a unified platform, generating vast amounts of data that necessitate effective business intelligence practices. The three fundamental aspects of the Internet of Things are connectivity, analysis, and integration. Firstly, establishing device virtualization and standardizing device integration with cloud-based IoT enterprise platforms enable seamless connections. As heterogeneous devices become part of the IoT network, they generate massive volumes of data. Therefore, robust and

high-speed messaging systems are crucial to ensure reliable, secure, and bidirectional communication between devices and the cloud. Secondly, integration entails managing device-to-device endpoint identities, maintaining metadata, and overseeing the entire lifecycle of each device. Lastly, real-time analysis of incoming and outgoing data streams requires various techniques such as aggregation, filtering, correlation, and processing to enhance system performance.

A. Smart Home Automation: Home automation refers to the capability of programming and scheduling events for IoT devices, allowing them to be remotely monitored and accessed using various communication protocols such as radio frequency (RF), Wi-Fi, Z-Wave, and Zigbee. This technology enables efficient energy consumption, time management, and cost savings. Home automation involves the integration of IoT-based smart devices, including smart light switches, security systems, electrical appliances, smart door locks, smart irrigation controllers, smart thermostats, wireless home energy monitors, and other internet-connected devices. These devices communicate with each other through waves of communication, facilitating seamless interaction and coordination. To implement a smart home automation system, technologies such as Arduino UNO and GSM modules are utilized to control home appliances and enable remote management [13].

B. Smart healthcares: IoT healthcare plays a crucial role in reducing the cost of patient care through the implementation of Wireless Medical Sensor Networks (WMSNs). By utilizing IoT detectors, patients can be easily tracked, and the location of doctors can be determined. To illustrate the significance of this technology, consider a scenario where a patient is at home connected to a cloud-based health monitoring system. If the patient experiences a health issue such as low heart rate or blood pressure, the cloud system, which is linked to the hospital, instantly transmits this information. The hospital receives complete details regarding the patient's condition and important information. They dispatch an ambulance to transport the patient back to the hospital. Upon arrival at the hospital, in emergency cases, all necessary prescriptions, medicines, and operation theaters are prepared in advance, and the doctors are fully informed about the patient's medical history and current condition. This level of transparency and information availability significantly reduces time and effort. The smart healthcare system minimizes human intervention, saves time, and optimizes resource utilization, leading to efficient and effective patient care.

C. Smart agriculture: In today's era, many countries are embracing IoT technology in the field of agriculture to improve food production, ensure safety, and streamline logistics and warehousing processes. IoT technology enables the collection of data and analysis of various factors such as crop diseases, weather forecasting, soil quality, integrated pest management, and control. Through remote crop monitoring, climate monitoring, and forecasting, IoT facilitates observation, inspection, identification, record tracking, and automatic spraying of pesticides at the appropriate time. Additionally, IoT plays a vital role in water management for agriculture as an adequate water supply is crucial for crop growth, while excess or shortage of water can harm crops. By leveraging sensors, data, and machinery, IoT enables precise water management and empowers farmers with real-time data related to the agricultural process. This research paper aims to explore the application of advanced technologies like remote sensing, Geographical Information System (GIS), and IoT in modern agriculture. Numerous IoT devices are deployed on farms to conduct surveys, collect data, and generate analytics reports through a dashboard. This real-time monitoring and decision support system, provided by the dashboard data, proves invaluable for optimizing field parameters and enhancing agricultural productivity.

- Soil parameters such as moisture and conductivity can be accurately determined using GPS-enabled devices and sensors. This allows farmers to optimize their harvesting process in alignment with the condition of the soil.
- Environmental parameters like temperature, humidity, light, and wind can be monitored through remote sensing technology. This data provides valuable insights into the environmental conditions that impact crop growth and development.
- Water quality parameters, including pH, conductivity, dissolved oxygen, and dissolved ions, can be detected using IoT devices. Farmers can conveniently check water levels in tanks and other storage systems through their mobile devices or desktops, ensuring proper water management.
- Weather parameters such as wind speed, atmospheric pressure, and wind direction are essential for making informed agricultural decisions. IoT technology enables the collection and analysis of real-time weather data, allowing farmers to anticipate weather patterns and adjust their farming practices accordingly.

D. Smart Energy and the Smart Grid: Smart Grid technologies are an integral component of the IoT framework, enabling the efficient management of various aspects such as lighting, traffic signals, parking spaces, power distribution, and traffic congestion through the utilization of IoT smart sensors. By leveraging IoT-enabled sensors, the Smart Grid system can collect real-time data from different sources, allowing for intelligent decision-making and optimization of energy resources. For instance, smart sensors embedded in lighting systems can adjust brightness levels based on environmental conditions, reducing energy consumption while ensuring adequate illumination. Traffic signals equipped with IoT sensors can dynamically adapt to traffic patterns, improving traffic flow and minimizing congestion. Moreover, IoT technology enables efficient management of parking spaces by

providing real-time information on availability. This allows drivers to quickly locate vacant parking spots, reducing unnecessary congestion and enhancing the overall parking experience. In the realm of power distribution, IoT sensors facilitate the monitoring of power influxes and enable proactive measures to prevent power outages and ensure a stable electricity supply. By collecting and analyzing data from various sensors, the Smart Grid system can optimize energy distribution, enhance grid reliability, and enable effective load management.

Overall, the integration of Smart Grid technologies within the IoT framework brings enhanced efficiency, sustainability, and improved quality of services across various domains, making cities smarter and more responsive to the needs of their inhabitants.

E. Smart Transportation and Mobility: The smart mobility ecosystem has the potential to revolutionize the traffic management landscape in India and transform the way goods are transported. By integrating sustainable and safe connectivity, connected vehicles can leverage the power of rapidly advancing technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI). Through IoT and AI, connected vehicles can establish seamless communication and exchange of data with infrastructure, other vehicles, and traffic management systems. This enables real-time monitoring and analysis of traffic conditions, allowing for intelligent routing and optimized traffic flow. With enhanced connectivity, traffic management can become more efficient, reducing congestion and travel time for commuters. Furthermore, the integration of IoT and AI in the smart mobility ecosystem enables predictive analytics and intelligent decision-making. Vehicles can gather data on road conditions, weather patterns, and traffic volumes, allowing for proactive measures to prevent accidents and improve overall safety. AI algorithms can analyze the data in real-time, identifying potential risks and providing timely warnings to drivers and authorities. In the context of goods transportation, smart mobility can streamline logistics operations and enhance supply chain efficiency. IoT-enabled tracking systems can monitor the location and condition of goods in transit, ensuring timely delivery and minimizing losses. AI-powered algorithms can optimize route planning, taking into account factors such as traffic conditions, fuel efficiency, and delivery deadlines. The convergence of smart mobility with IoT and AI technologies holds immense potential for transforming the Indian traffic management scenario and revolutionizing the movement of goods. By embracing sustainable and connected solutions, India can create a safer, more efficient, and environmentally-friendly transportation ecosystem[11].

F. Smart Factory and Smart Manufacturing: The digital transformation of manufacturing technology and operational technology represents a significant advancement in the realm of Industrial Internet of Things (IoT). With the integration of smart sensors in machinery within a smart factory, data is automatically generated, providing valuable insights for better decision-making and improved production outcomes. This era of the Fourth Industrial Revolution, commonly known as Industry 4.0, enables the generation of real-time data from physical assets within the factory environment. This data empowers manufacturers to efficiently manage their assets, enhance production efficiency, monitor the quality of manufactured materials, and prioritize worker safety. By leveraging the data collected from smart sensors, manufacturers can gain deep insights into various aspects of their operations. Real-time monitoring allows for proactive maintenance, reducing downtime and optimizing overall equipment effectiveness. Furthermore, data analysis enables the identification of bottlenecks and inefficiencies in the production process, leading to targeted improvements and increased productivity. In addition to operational benefits, the integration of IoT technologies enhances quality control in manufacturing. By continuously monitoring and analyzing the quality of materials being produced, manufacturers can quickly identify and rectify any deviations or defects. This ensures that only high-quality products reach the market, enhancing customer satisfaction and brand reputation. Worker safety is also prioritized in the digital transformation of manufacturing. IoT-enabled technologies provide real-time monitoring of workplace conditions, detecting potential hazards and improving safety protocols. This leads to a safer working environment and reduces the risk of accidents or injuries [12].

G. Smart Environment: The Internet of Things (IoT) revolutionizes our surroundings by seamlessly connecting physical objects to the virtual world through the exchange of information, facilitated by Radio-Frequency Identification (RFID) technology. In the context of IoT, RFID acts as an asymmetric system, enabling the mapping and control of objects through the use of tags that contain unique Electronic Product Codes (EPCs). RFID technology plays a pivotal role in enabling connectivity and interaction within the IoT ecosystem. Each object is equipped with an RFID tag that stores relevant information, such as its identity or characteristics. These tags can be scanned and read by RFID readers, allowing for efficient data collection and communication between the physical object and the virtual world. The uniqueness of the Electronic Product Code (EPC) associated with each RFID tag ensures precise identification of the target object. By

utilizing this identification mechanism, IoT systems can track and manage a wide range of objects, from consumer products to industrial equipment, in a seamless and automated manner.

The exchange of information between physical objects and the virtual world opens up new possibilities for enhancing efficiency, automation, and decision-making. Real-time data collected through RFID-enabled IoT systems enables businesses and individuals to gain valuable insights into object location, usage patterns, and operational status. This information can be leveraged to optimize processes, improve resource allocation, and enhance overall productivity. In addition, RFID technology in the IoT offers numerous benefits, such as enhanced supply chain management, inventory control, and asset tracking. By leveraging RFID-enabled systems, businesses can streamline operations, reduce errors, and improve the accuracy and speed of data collection. Internet of Things creates a smart environment where physical objects are seamlessly connected to the virtual world. Through the use of unique Electronic Product Codes and RFID tags, objects can be accurately identified, monitored, and managed, opening up a world of opportunities for improved efficiency, automation, and data-driven decision-making.

H. Smart Education: Smart learning environments have revolutionized education by incorporating e-gadgets that offer flexibility, efficiency, and a seamless learning experience for researchers, educators, and students across various disciplines. These innovative environments enable individuals to access educational resources anytime and anywhere, transforming the traditional classroom into a virtual learning space. E-gadgets such as tablets, laptops, and mobile devices are at the core of smart learning environments, providing users with the tools and technologies necessary for enhanced learning experiences. These devices offer a wide range of educational resources, interactive materials, and multimedia content that cater to individual learning styles and preferences [14].

I. Smart wearable: Wearable devices have emerged as lightweight, versatile, and customizable gadgets that bridge the gap between the human body and the "Internet of Things" (IoT) ecosystem. These devices include smart glasses and virtual reality headsets, allowing users to seamlessly connect and interact with the digital world.

One of the key features of wearable devices is their ability to monitor various physiological parameters in real-time. Body area sensors embedded in these devices can track vital information such as body temperature, movement patterns, and pulse rate. This continuous monitoring enables individuals to gain insights into their health and well-being, leading to better self-awareness and proactive healthcare management. To facilitate seamless connectivity and data transmission, wearable devices leverage technologies such as Bluetooth Low Energy (BLE). This energy-efficient wireless protocol enables the transfer of sensor data from the wearable device to an IoT-connected gateway. From there, the data can be processed, analyzed, and stored in the cloud infrastructure with the support of big data technologies. The integration of wearable devices with the IoT ecosystem opens up a world of possibilities. These devices can be used for various applications, including fitness tracking, remote patient monitoring, virtual reality experiences, and augmented reality applications. The data collected from wearable devices can provide valuable insights for healthcare professionals, researchers, and individuals striving for improved performance and well-being. The lightweight and customizable nature of wearable devices makes them suitable for a wide range of use cases and user preferences. Whether it's a smartwatch, fitness band, or augmented reality headset, these devices offer a personalized and immersive experience tailored to the user's needs.

III. SECURITY OF IOT DEVICES:

Securing IoT devices is of paramount importance to safeguard them against potential vulnerabilities and cyber-attacks. While the golden ratio, also known as the golden mean or golden section, holds mathematical significance in diverse disciplines, it does not directly pertain to the security of IoT devices. The golden ratio is a mathematical concept that relates to the aesthetic and harmonious proportions found in art, architecture, and nature. It does not possess inherent capabilities to address the complex security challenges faced by IoT devices. To ensure the security of IoT devices, it is essential to implement robust measures such as strong authentication protocols, encryption algorithms, secure communication channels, and regular software updates. Additionally, adopting industry best practices, adhering to security standards, conducting vulnerability assessments, and implementing intrusion detection systems are vital steps to fortify the security of IoT devices. Cyber security in the context of IoT devices involves protecting them from potential threats such as unauthorized access, data breaches, malware attacks, and privacy breaches. It requires a comprehensive approach that encompasses both hardware and software security measures. By employing state-of-the-art security technologies, following security guidelines, and staying updated with the latest security patches and updates, organizations and individuals can enhance the security posture of their IoT devices. This proactive approach is crucial to mitigating risks and maintaining the integrity, confidentiality, and availability of IoT systems and the data they handle.

In summary, while the golden ratio has its significance in various domains, it does not directly relate to the security of IoT devices. Protecting IoT devices necessitates implementing robust security measures, adhering to best practices, and

staying vigilant against emerging threats in the dynamic landscape of cybersecurity.

A. Sensor Device Security: Internet of Thing uses various kinds of sensors may be wearable, implantable or portable, and integrated with the different wireless communication system. These wireless sensors will generate massive amounts of data which must be secured from security attacks. By applying the hybrid cryptography technique for hardware and connected devices to protect from intruder.

B. IoT Network Security: the detection of misbehaving devices by observing abnormal traffic patterns deriving a suitable policy for background data transfer by analysis of, for example, traffic volume, congestion level, load status information in the specific network area

C. Cloud Security: The huge amount of data generated through various types of IoT Devices. As the continuously increase the massive data of IoT interaction on cyber world, for the smooth processing and analysis of big data,, novel hybrid technique is used for transform raw data into smart data .so by applying adaptive machine learning efficient algorithm for all the things that can make decision easily. To improve the IoT framework performance by data mining, machine learning by extracting the meaningful smart data patterns generated by IoT and makes them more intelligent. On cloud processing of high volumes big data generated by sensors in a repetitive manner is really a big challenge to monitor, manage, optimize and analyze.

D. Authentication and Authorization: Implementing a robust authentication and authorization mechanism is essential to prevent unauthorized access to IoT devices. The use of strong encryption protocols and secure keys strengthens device authentication in 5G networks. Two-factor authentication and multi-factor authentication add an extra layer of security, ensuring only authorized devices can connect

E. Encrypted Communication Channels: Securing data transmission between IoT devices and the 5G network is vital to protect sensitive information from interception or tampering. End-to-end encryption techniques like Transport Layer Security (TLS) or Secure Sockets Layer (SSL) ensure that data remains confidential and integral during transmission.

F. Regular Firmware and Software Updates: Keeping IoT device firmware and software up to date is crucial to address vulnerabilities and security loopholes. Manufacturers should provide regular updates that include security patches. Automated update mechanisms simplify the process and ensure devices receive the latest security enhancements promptly.

G. Access Controls and Permissions: Implementing strong access control measures restrict unauthorized access to IoT devices, ensuring a secure network. Role-based access control (RBAC) or attribute-based access control (ABAC) allow administrators to assign specific privileges to users and devices. Network segmentation prevents compromised devices from affecting the entire IoT ecosystem.

H. Intrusion Detection and Prevention Systems: Deploying Intrusion Detection and Prevention Systems (IDPS) plays a vital role in real-time detection and mitigation of security breaches. These systems monitor network traffic, analyze patterns, and raise alerts when suspicious activities occur. IDPS helps prevent unauthorized access, data leakage, and other security incidents, enhancing IoT device safety.

I. Physical Security Measures: Physical security measures are often overlooked but are equally important in protecting IoT devices. Measures like tamper-evident packaging, secure storage, and restricted physical access prevent unauthorized tampering or theft. Unique identifiers or serial numbers aid in tracking and tracing devices, enhancing overall security.

J. Regular Security Audits: Regular security audits are crucial for identifying vulnerabilities and ensuring continuous improvement in IoT device security. Comprehensive security assessments, penetration testing, and vulnerability scans help identify potential weaknesses. Remedial actions can be taken based on audit findings to strengthen IoT device security.

IV. Standard Security Architecture For IoT And 5G:

The Advanced IoT Security Framework aims to create a secure environment where IoT devices can effectively sense information and detect any malicious behavior or threats. In the context of 5G communication technology, security and privacy in the Internet of Things (IoT) rely on the access architecture of wireless systems and the interaction with distributed storage units for data collection. Securing IoT devices is paramount to protect them from potential vulnerabilities and cyber-attacks. While the golden ratio, also known as the golden mean or golden section, holds mathematical significance in various fields, it is not directly applicable to IoT device security[6].

To enhance IoT security, the following measures should be implemented:

1. Monitoring and Logging: Establish monitoring and logging mechanisms to track and identify suspicious activities or anomalies in IoT device behavior. This allows for the timely detection and response to potential security breaches.
2. Physical Security: Protect physical access to IoT devices by implementing appropriate measures. This includes securing the physical location of the devices, using tamper-evident seals, and restricting physical access to authorized personnel only.
3. Secure Communication Protocols: Utilize secure communication protocols such as Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) to encrypt data transmission between IoT devices and the network. This ensures the confidentiality and integrity of data during transit.
4. Device-to-Device and Device-to-Cloud Communication: Implement secure protocols for both device-to-device and device-to-cloud

communication. This ensures that data exchanged between IoT devices and the cloud is protected from unauthorized access and tampering.

By implementing these security measures, organizations can significantly enhance the security posture of their IoT devices. It is crucial to stay updated with the latest security practices, regularly apply security patches and updates, and conduct periodic security assessments to mitigate risks and protect IoT devices from potential threats.

V. Database Server Security Of Arduino Uno, Zigbee And Gsm Using Thingspeak:

Speathing is powerful open-source software designed for IoT-enabled applications. It offers the capability to store IoT data on the cloud through an API interface with port 80. To analyze and test the sensor data, MATLAB analytics is utilized by creating dedicated channels on the cloud for each type of sensor data. Security is a critical aspect of Speathing, and it incorporates a hybrid AES crypto analysis technique to ensure data confidentiality and integrity. This technique leverages the mathematical significance of the golden prime ratio, providing a high level of security for various components of IoT devices [2].

The software ensures robust security measures for software applications, hardware sensors, firmware, configuration files, security policies, network activities, device identification, IP address tracing, user behavior, and file system protection. By implementing these security features, Speathing aims to safeguard the IoT ecosystem and protect sensitive information from unauthorized access or malicious attacks. Furthermore, the software emphasizes the confidentiality of the API key, which serves as a unique identifier for secure communication between the IoT devices and the cloud platform. This confidential API key ensures that only authorized entities can access and interact with the IoT data stored on the cloud. Speathing provides an open-source solution for IoT applications, facilitating data storage on the cloud through an API interface. It employs MATLAB analytics for regression testing of sensor data and incorporates hybrid AES crypto analysis with the golden prime ratio for robust security. By offering comprehensive security measures, Speathing aims to protect various aspects of IoT devices and ensure the privacy and integrity of IoT data [4].

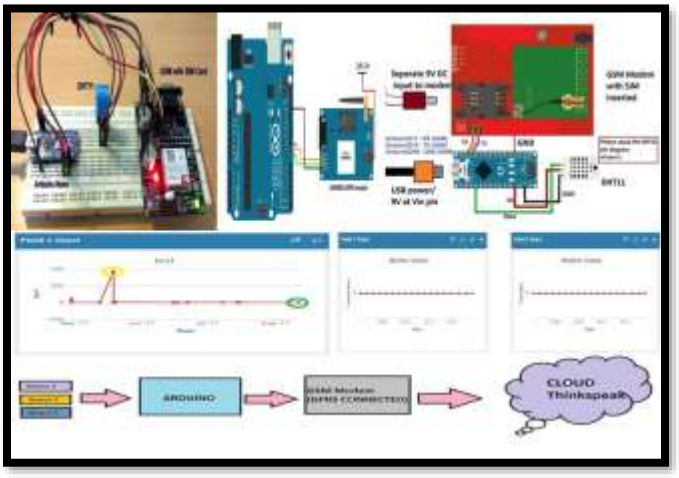

Fig. 1 Thingspeak Server- IoT sensor data on Cloud

An advanced cryptographic analysis technique based on the "golden prime ratio" is employed in the IoT security framework to establish a secure environment. This framework enables IoT devices to efficiently perceive information and detect any anomalous or malicious behavior in the face of threats, cyber-attacks, and contextual attacks. The security code is concealed within the sensor data and undergoes significant transformations. The golden prime ratio, derived from the concept of a golden rectangle, plays a pivotal role in the cryptographic process. When a golden rectangle with a longer side, denoted as "a," and a shorter side, denoted as "b," is placed adjacent to a square with sides of length "a," it generates another golden rectangle with longer side "a + b" and shorter side "a." This relationship, along with the golden ratio's association with right-angled triangles and the Fibonacci sequence, contributes to the development of a faster and more efficient cryptosystem. By leveraging the mathematical properties of the golden prime ratio, the IoT security framework enhances the security of IoT devices. It enables the detection and prevention of potential threats and attacks, ensuring the integrity and confidentiality of the system [5].This technique offers efficient outcomes and contributes to the development of robust and reliable cryptographic systems within the IoT domain. The utilization of the golden prime ratio in an advanced cryptographic analysis technique strengthens the IoT security framework. By incorporating this mathematical concept, IoT devices can effectively sense and identify threats, malicious behavior, and contextual attacks. The application of the golden prime ratio, along with its relationships to right-angled triangles and the Fibonacci sequence, facilitates the development of faster and more secure cryptosystems for IoT environments.

TABLE I
GOLDEN PRIME RATIO

1.618034 Phi (Φ)	Index of Seed	Distance From Centre	Theta Angle (Θ)	X-Axiz	Y-Axiz
222.4922	1	1	0	1	0
137.5078	2	1.414213562	137.5078	-1.0428	0.955288
	3	1.732050808	275.0155	0.151426	-1.72542
	4	2	412.5233	1.216878	1.587202
	5	2.236067977	550.0311	-2.20189	-0.38948
	6	2.449489743	687.5388	2.06677	-1.31471
	7	2.645751311	825.0466	-0.68685	2.555042
	8	2.828427125	962.5544	-1.30364	-2.51008
	9	3	1100.062	2.817964	1.029117
	10	3.16227766	1237.57	-2.92304	1.206587
	11	3.31662479	1375.078	1.405739	-3.00398
	12	3.464101615	1512.585	1.036749	3.305322
	13	3.605551275	1650.093	-3.11956	-1.80785
	14	3.741657387	1787.601	3.654386	-0.80341
	15	3.872983346	1925.109	-2.22747	3.168341

Utilizing the principles of the Golden Ratio (Φ), a cryptographic system can be devised to accurately determine the right angle of any given object, as illustrated in the following example:

The Golden Ratio, denoted as Φ, is a mathematical constant approximately equal to 1.6180339887. It is often represented by the Greek letter Phi (Φ) and holds significant mathematical properties. One of its notable characteristics is its relationship with the Fibonacci sequence, where each number in the sequence is the sum of the two preceding numbers.

To create a cryptosystem for calculating the right angle of an object, we can employ the Golden Ratio as follows:

1. Gather precise measurements of the object's sides or angles.
2. Apply the Golden Ratio to determine the length of one side of a right-angled triangle.
3. Use this derived length and the measured lengths of the other two sides to calculate the object's right angle.

By utilizing the mathematical properties of the Golden Ratio, this cryptosystem enables accurate determination of the right angle of various objects. The Golden Ratio's inherent relationship with the Fibonacci sequence contributes to the reliability and precision of the calculations.

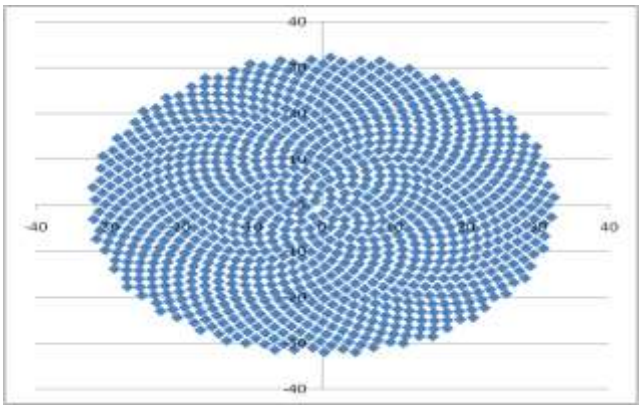

Fig. 2 Golden Prime Ration Functional Values

The golden ratio is widely recognized as one of the most irrational numbers, possessing unique mathematical properties. When employed with higher decimal place accuracy, the golden ratio becomes an appealing tool for generating more secure keys. Golden Prime Ratio cryptography offers a solution to address the vulnerabilities associated with chosen-plaintext attacks, thereby finding extensive applications in secret key generation. The golden ratio, symbolized by Φ and approximately equal to 1.6180339887, holds significance in various fields due to its intriguing characteristics. In the realm of cryptography, leveraging the golden ratio in key generation can result in keys with enhanced security. Golden Prime Ratio cryptography specifically focuses on mitigating the insecurities stemming from chosen-plaintext attacks. These attacks occur when an adversary possesses the ability to select specific plaintexts and observe their corresponding cipher texts. By incorporating mathematical operations based on the golden ratio, Golden Prime Ratio cryptography offers countermeasures against such attacks, bolstering the security of the generated keys. The application of Golden Prime Ratio cryptography extends to a wide range of scenarios where secret key generation is paramount. By harnessing the distinctive properties of the golden ratio, this cryptographic approach provides an additional layer of protection against chosen-plaintext attacks, thereby strengthening the overall security of secret key generation processes. While Golden Prime Ratio cryptography offers advantages in generating secure keys, it is important to emphasize that comprehensive security measures should involve a holistic approach. Incorporating established cryptographic algorithms, protocols, and best practices alongside Golden Prime Ratio cryptography ensures a robust and comprehensive security framework. The golden ratio, known for its irrationality, can be utilized with higher decimal place accuracy to generate more secure keys. Golden Prime Ratio cryptography addresses vulnerabilities associated with chosen-plaintext attacks and finds extensive applications in secret key generation. By integrating the golden ratio into cryptographic processes, a higher level of security can be achieved, enhancing the overall protection of sensitive information.

VI. CONCLUSION:

The emergence of 5G technology presents tremendous opportunities for the Internet of Things (IoT), but it also calls for careful preparation and groundwork from device manufacturers. While the potential benefits of IoT with 5G are vast, it is crucial to prioritize the safety and security of connected devices. Implementing robust safety measures such as authentication, encrypted communication, regular updates, access controls, intrusion detection, physical security, and security audits is essential. By incorporating these measures, we can establish a resilient IoT ecosystem that capitalizes on the potential of 5G while effectively addressing emerging threats. Furthermore, exploring the application of the golden ratio in enhancing IoT device security is a promising avenue. This paper delves into the realm of encryption techniques and prime-based algorithms to bolster the confidentiality and integrity of IoT device communications. By leveraging these methods, we can strengthen the protection against unauthorized access and mitigate potential vulnerabilities. Ensuring the safety and security of IoT devices in the era of 5G requires a multi-faceted approach[7]. It involves implementing comprehensive safety measures and exploring innovative techniques such as encryption and prime-based algorithms. By diligently addressing these aspects, we can foster a secure and trustworthy IoT environment that fully utilizes the potential of 5G technology.

REFERENCES

[1] Arun Madhu, A. S. (n.d.). Wireless Sensor Network Security in Military Application using Unmanned Vehicle. *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)* , 51-58.

[2] Dr.A.A.Gurjar, N. A. (2018). Heart Attack Detection By Heartbeat Sensing using Internet Of. *International Research Journal of Engineering and Technology (IRJET)* .

[3] Ernest Ezema, A. A. (2018). Open Issues and Security Challenges of Data Communication Channels in Distributed Internet of Things (IoT): A Survey. *ResearchGate* , 12.

[4] Ezema, E., Abdullah, A., & Mohd, N. F. (2018). Open Issues and Security Challenges of Data Communication Channels in Distributed Internet of Things (IoT): A Survey. *Circulation in Computer Science* , 22-32.

[5] Kajal R.K Pandey, K. A. (2018). Improvement and Enhancement in Emergency Medical Services using IOT. *International Research Journal of Engineering and Technology (IRJET)* , 4.

[6] L. Militano1, G. A. (2015). Device-to-Device Communications for 5G Internet of. *Araniti et al., licensed to ICST* , 15.

[7] Ms. Reshma S. Sapakal #1, M. S. (2013). 5G Mobile Technology. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* , 4.

[8] Nadeem Javaid, A. S. (October 2018). Intelligence in IoT-Based 5G Networks:Opportunities and Challenges. *IEEE Communications Magazine* , 100.

[9] Pirinen, P. (2014). A Brief Overview of 5G Research Activities. *ResearchGate* , 7.

[10] Ramão Tiago Tiburski, L. A. (2016). Security Challenges in 5G-Based IoT. *Springer International Publishing Switzerland* , 21.

[11] Sagar D. Charde, P. N. (2018). A METHODOLOGY: IOT BASED DROWSY DRIVING WARNING AND TRAFFIC COLLISION INFORMATION SYSTEM. *International Research Journal of Engineering and Technology (IRJET)* , 3.

[12] Sapna Suryawanshi, R. B. (2018). Waste Management System Based On IoT. *International Research Journal of Engineering and Technology (IRJET)*, 3.

[13] Siddharth Wadhwani, U. S. (2018). Smart Home Automation and Security System using Arduino and IOT. *International Research Journal of Engineering and Technology (IRJET)*, 3.

[14] Somnath D. Bhagwat, A. I. (2018). Smart Green House using IOT and Cloud Computing. *International Research Journal of Engineering and Technology (IRJET)*, 4.

AUTHORS

About the Author –

Prithviraj Singh is pursuing Ph.D. in Computer Science and an expert in the field of VANET and IoT security. He is currently a faculty member in the Department of Computer Science at GOKUL GLOBAL UNIVERSITY, where he leads research initiatives in cyber security and IoT technologies. Mr. Prithviraj Singh Solanki has research interests in M/L algorithms include encryption techniques, network security, and privacy in IoT systems. He has published several papers in reputable journals and has presented his work at international conferences.

✉ prithvisingh2488@gmail.com