ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

BLOCK QUANTUM COMPUTING FOR SECURE SATELLITE COMMUNICATION

Saranya R
CSE
Paavai College of Engineering
Namakkal,TamilNadu
rsarancse@gmail.com

Aswin C
CSE
Paavai College of Engineering
Namakkal,TamilNadu
aswinraja281@gmail.com

Santhosh M
CSE
Paavai College of Engineering
Namakkal,TamilNadu
santhoshmms4285@gmail.com

Arjun P
CSE
Paavai College of Engineering
Namakkal,TamilNadu
arjunprathap30@gmail.com

Harishjeyaraj D
CSE
Paavai College of Engineering
Namakkal,TamilNadu
harishjeyraj11092002@gmail.com

ABSTRACT-Satellite communication networks have gained a lot of attention recently as a solution to mitigate the limitations of terrestrial networks such as stability and coverage. Due to satellite physical constraints in terms of available power and area, data processing capacity is low, storage and security are limited such that the data may be vulnerable to tampering or contamination by attackers. Since satellite communication has been more and more important in developing global communication networks, there have been concerns about the security in satellite communication. It is a challenge to protect satellite network from illegal information access and use storage space effectively. The integration of satellite systems with smart computing and networking technologies, such as Blockchain and Quantum Computing, has intensely augmented sophisticated cyberattacks against satellite environments. In this project, a blockchain technology and Quantum Key Distribution QKD protocol based on authentication and privacy protection scheme is proposed for a satellite communication network. to this aim, an architecture consisting of both conventional and restricted devices connected to the blockchain via a wireless heterogeneous network is deployed. Secure communications by introducing the variant of pre-quantum RSA called lattice-based RSA generates quantum key pool (QKP) to relay keys for ground stations device and satellites. The communication is carried out through registration, authentication and revocation. In this scheme, the satellite will forward the collected information to the ground base station, which will record all key parameters on the distributed blockchain and all malicious node certificates will be cleared from the blockchain by the ground base station. The proposed satellite-based Blockchain and Quantum Key Distribution system provides high security level for the coming 6G and beyond networks, the Internet of things, self-driving cars, and other fast-developing applications.

I. INTRODUCTION

A. Overview

A satellite is a body that orbits around another body in space. There are two different types of satellites – *natural and man-made*. Examples of natural satellites are the Earth and Moon. The Earth rotates around the Sun and the Moon rotates around the Earth. A man-made satellite is a machine that is launched into space and orbits around a body in space.

Figure 1.1. Satellite

Man-made satellites come in many shapes and size and have different pieces of instruments on them to perform different functions while in space.

1) Satellite Communication

Satellite communication is the method of transporting information from one place to another using a communication satellite in orbit around the Earth. Watching the English Premier League every weekend with your friends would have been impossible without this. A communication satellite is an artificial satellite that transmits the signal via a transponder by creating a channel between the transmitter and the receiver located at different

locations on the Earth. Telephone, radio, television, internet, and military applications use satellite communications. Believe it or not, more than 2000 artificial satellites are hurtling around in space right above your heads.

2) Satellite Communications in India

It's interesting to know that the Indian National Satellite (INSAT) system is one of the largest domestic communication systems that is placed in the geo-stational orbit. There are more than 200 transponders in the INSAT system and are used for various purposes such as telecommunications, weather forecasting, television broadcasting, disaster warning, search and rescue operations, and satellite newsgathering.

Below is the list of communication satellites along with their applications:

3) Types of Satellite Network

Satellites can be classified by their function since they are launched into space to do a specific job. The satellite must be designed specifically to fulfil its role. There are nine different types of satellites i.e. Communications Satellite, Remote Sensing Satellite, Navigation Satellite, LEO, MEO, HEO, GPS, GEOs, Drone Satellite, Ground Satellite, Polar Satellite. Communications satellites are artificial satellites that relay receive signals from an earth station and then retransmit the signal to other earth stations. They commonly move in a geostationary orbit. A remote Sensing instrument collects information about an object.

- Communication satellites

Their purpose of them is to serve as a relay station in the space using radio frequency waves to transmit the signal and information with it.

- Navigation satellites

The radio line signals sent from navigation satellites with the help of regularly developed electronic equipment enables the signals receiver on the earth to identify its position with pretty high accuracy.

- Earth observation satellites

These satellites are constructed with the goal to observe the earth from the space in order to monitor environmentally, make maps, use for meteorology, but usually not for military purposes.

- Astronomical satellites

The galaxies, other planets and other space bodies can be tracked and studied with the help of these satellites.

- Reconnaissance satellites

They are similarly as Earth Observation satellites are also used to watch the earth, but for military and intelligence (e. g. espionage) purposes. Governments do not provide much information about the power of these satellites as it used for various secret purposes.

- Solar power satellites

They use the radio frequency waves to transmit the power of sun to a huge antenna on the earth. The solar power afterwards can be used as a resource instead of traditional power.

- Space stations

The purpose of man shaped space stations is to create an environment for more and longer different scientific researches in comparison with other spacecrafts to measure the effects for human beings of a longer stay in the space.

- Weather satellites

Space vehicles are used to observe the weather and, in some case, the global climate.

- Miniaturized satellites

These satellites have uncommonly light weight and are very small (e.g., 500 – 10 kg compared with traditional satellites, which can weight about 5000 kg, like PAS 1 – R made by Pan Am Sat Corp.). The advantage of such spacecrafts is the much lower requirements for equipment in order to launch them into space, which leads to much lower costs. Besides that, they are also used for the missions, which usual satellites are not able to execute, like the low data rate transmission constellations, inspection of traditional space vehicles and etc. [2] discussed about a method, This scheme investigates a traffic-light-based intelligent routing strategy for the satellite network, which can adjust the pre-calculated route according to the real-time congestion status of the satellite constellation. In a satellite, a traffic light is deployed at each direction to indicate the congestion situation, and is set to a relevant color, by considering both the queue occupancy rate at a direction and the total queue occupancy rate of the next hop. The existing scheme uses TLR based routing mechanism based on two concepts are DVTR Dynamic Virtual Topology Routing (DVTR) and Virtual Node (VN). In DVTR, the system period is divided into a series of time intervals. On-off operations of ISLs are supposed to be performed only at the beginning of each interval and the whole topology keeps unchanged during each interval. But it has delay due to waiting stage at buffer. So, this method introduces an effective multi-hop scheduling routing scheme that considers the mobility of nodes which are clustered in one group is confined within a specified area, and multiple groups move uniformly across the network. [3] proposed a system, in which a predicate is defined for measuring the evidence for a boundary between two regions using Geodesic Graph-based representation of the image. The algorithm is applied to image segmentation using two different kinds of local neighborhoods in constructing the graph. Liver and hepatic tumor segmentation can be automatically processed by the Geodesic graph-cut based method. This system has concentrated on finding a fast and interactive segmentation method for liver and tumor segmentation. In the preprocessing stage, the CT image process is carried over with mean shift filter and statistical thresholding method for reducing processing area with improving detections rate. Second stage is liver segmentation; the liver region has been segmented using the algorithm of the proposed method. The next stage tumor segmentation also followed the same steps. Finally the liver and tumor regions are separately segmented from the computer tomography image.

- Biosatellites

In order to conduct the scientific tests and various experiments with the different living forms, the biosatellites were created.

- Killer Satellites

They are also named Anti-Satellite Weapons and are used for destruction of rival satellites or other weapons in orbits.

4) Satellite orbits

In general, orbit is described as a pathway, which one space body makes around the other space body, because they are both influenced by gravity and centripetal force. The orbits, where satellites are launched by rockets, differ according their altitude above the surface of Earth and are most often categorized into the following classes:

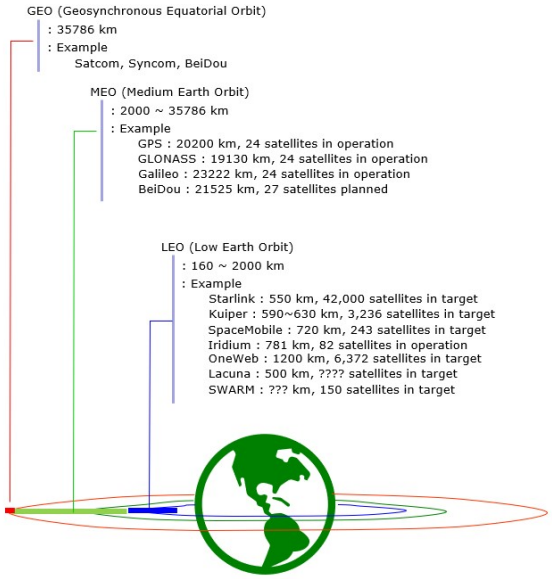

Figure 1.2. Satellite Orbits

- Low Earth Orbit (LEO)

LEO finds its place from 200 km to 1200 km height above the earth. The advantage of this orbit is the shorter signal traveling time and lower possibility to lose its path. On the other hand, the coverage zone is quite small (in comparison with GEO) and the connection to satellite from ground station time is shorter, because the satellite moves quicker as the earth is turning. The increased interest in mobile communications via satellites over the last years motivated the augmentation of LEO usage and development of them.

- Medium Earth Orbit (MEO)

MEO is located between 1200 km and 35286 km altitude above earth surface. Some literature sources indicate that the Medium Earth Orbit is located between 5000 km and 13000 km height or between two Van Allen belts [Walke00]. Van Allen belts are two high intensity radiation zones of the earth, where highly charged particles and high energy neutrons take place. For this reason, the two belts are communication satellites damaging. Thus, it is avoided to place the satellite in the Van Allen belts zones.

- Highly Elliptical Orbit (HEO)

The name of the HEO arises from its elliptical form, which is helpful in order to achieve a better coverage of higher populated zones or usually not reachable parts of earth (such as poles) without the interruption of lower orbits.

- Geostationary Orbit (GEO)

GEO is placed 35786 km above Earth's surface. The orbit is called geostationary orbit, because satellites', placed in this orbit, speed is matched with earth turning speed so that the satellite moves always together with the earth. In other words, to say, if the one would be able to see the satellite from the earth, the satellite would always stay in the same point of the space from the earth perspective. Most of the communication satellites are place in GEO.

5) Satellite Applications

The applications of satellite communication systems include the following.

- TV
- Telephone
- Monitoring of Weather Condition and Forecasting
- Military
- Navigations
- Amateur Radio
- TV broadcasting like DTH (Direct to Home)
- Radio Broadcasting
- Remote sensing applications
- Disaster Management
- Voice communications & Radio Broadcasting
- Internet Access
- Digital cinema
- Internet applications to provide the application of internet connection for GPS applications, data transfer, Internet surfing, and many more.

B. Problems Identified

SATCOMs are particularly prone to eavesdropping due to the broadcast nature of the wireless medium and the very large coverage area.

- Traffic redirection attack

The attacker may send a fake binding update message to the CN claiming that a node (victim) has changed its care-of address due to its movement to a new location. Consequently, the CN will start sending packets to the new CoA and the victim node will not get any traffic.

- Man-in-the-middle attack

The attacker might sends poofed binding update message to the CN telling it to update the cacheen try to its own(attacker's) IP address. Consequently, the CN will start sending the packets to the attacker instead of the Satellite. The attacker may learn the confidential information of the message, may modify the packet before forwarding it to the Satellite. Thus, the attacker might act as a man-in-the-middle getting the all-important private data destined to the victim satellite (device)without the knowledge of the concerned parties. Moreover, the attacker can send modified control and command messages to the satellite, thereby altering the operation sequence of the satellite. This may lead to dangerous impact on the whole satellite communication systems.

- Bombing attack

In this type of attack, huge amount of unsolicited data traffic is flooded towards the victim node (Satellite), resulting in the bandwidth wastage as well as performance degradation. The attacker may exploit real-time streaming servers for this kind of attack. First, the attacker establishes a connection with streaming server, and starts to download a stream of data. After getting the sequence number, the attacker might claim that it has moved to a new location. The attacker might use the IP address of the victim (Satellite) in the binding update. As a result, subsequent packets from the server will be directed to the victim node that has not even requested any data from the server.

- Reflection attack

In some earlier design, CN could initiate route optimization signalling whenever CN receives packet through HA, and this may lead to reflection attack. Route optimization was initiated to the address that was included in the Home Address option. An attacker can take advantage of this and can send traffic with a care-of-address of the victim and the victim's address in the Home Address option, thereby redirecting route optimization signaling to the victim.

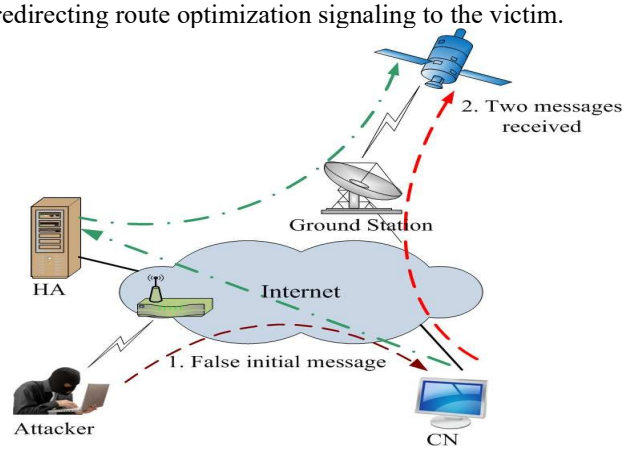

Fig.1.3. Reflection attack.

- Home Agent poisoning

Home Agent keeps the mapping of home address to Care-of-Address of the MH. Therefore, in every subnet crossing location updates are sent to HA to update the database entry accordingly. The entry can be corrupted if spoofed BU is accepted by the HA. This will affect all subsequent communication with that host whose entry has been corrupted and no Internet node will be able to reach the victim node.

- Resource exhaustion

Attacker establishes connections with the IP-enabled device on board the Satellite with thousands of fake IP addresses. Consequently, whenever the MH (Satellite) moves to some new location, it has to send to send BUs to all these imaginary hosts, thus huge processing power of the victim MH is wasted while dealing with these unnecessary BUs. This attack cannot be prevented with authenticated BUs.

- Attack on security protocols

The attacker may trick the MH to participate in unnecessary complex cryptographic operations, using up the resources. This is sometimes directed to the security mechanisms on the mobility protocols. Another kind of flooding attack can target the MH or CN to induce authentic but unnecessary binding updates and this type of attack is possible regardless of authentication protocol. The worst thing is that this attack on security protocols becomes severe for strong and expensive protocols.

These kinds of attack are very harmful for spacecrafts since they have limited processing power and unnecessary strong cryptographic operations may lead to denial-of-service attacks. The satellites may not able to do legitimate operation due to the execution of such expensive operations and the satellite communication may be disrupted as the satellite may become the single point of failure.

C. Cryptography

Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries.

Cryptography provides for secure communication in the presence of malicious third-parties—known as adversaries. Encryption uses an algorithm and a key to transform an input (i.e., plaintext) into an encrypted output (i.e., ciphertext). A given algorithm will always transform the same plaintext into the same ciphertext if the same key is used. Algorithms are considered secure if an attacker cannot determine any properties of the plaintext or key, given the ciphertext. An attacker should not be able to determine anything about a key given a large number of plaintext/ciphertext combinations which used the key.

1) Types of Cryptography

Cryptography can be broken down into three different types:

- Secret Key Cryptography
- Public Key Cryptography
- Hash Functions

Secret Key Cryptography, or symmetric cryptography, uses a single key to encrypt data. Both encryption and decryption in symmetric cryptography use the same key, making this the easiest form of cryptography. The cryptographic algorithm utilizes the key in a cipher to encrypt the data, and when the data must be accessed again, a person entrusted with the secret key can decrypt the data. Secret Key Cryptography can be used on both in-transit and at-rest data, but is commonly only used on at-rest data, as sending the secret to the recipient of the message can lead to compromise.

Examples:

- AES
- DES
- Caesar Cipher

Public Key Cryptography, or asymmetric cryptography, uses two keys to encrypt data. One is used for encryption, while the other key can decrypt the message. Unlike symmetric cryptography, if one key is used to encrypt, that same key cannot decrypt the message, rather the other key shall be used.

One key is kept private, and is called the "private key", while the other is shared publicly and can be used by anyone, hence it is known as the "public key". The mathematical relation of the keys is such that the private key cannot be derived from the public key, but the public key can be derived from the private. The private key should not be distributed and should remain with the owner only. The public key can be given to any other entity.

Examples:

- ECC
- Diffie-Hellman
- DSS

Hash functions are irreversible, one-way functions which protect the data, at the cost of not being able to recover the original message. Hashing is a way to transform a given

string into a fixed length string. A good hashing algorithm will produce unique outputs for each input given. The only way to crack a hash is by trying every input possible, until you get the exact same hash. A hash can be used for hashing data (such as passwords) and in certificates.
Some of the most famous hashing algorithms are:

1. MD5
2. SHA-1
3. SHA-2 family which includes SHA-224, SHA-256, SHA-384, and SHA-512
4. SHA-3
5. Whirlpool
6. Blake 2
7. Blake 3

2) Quantum Cryptography

Quantum cryptography is a science that applies quantum mechanics principles to data encryption and data transmission so that data cannot be accessed by hackers – even by those malicious actors that have quantum computing of their own. The broader application of quantum cryptography also includes the creation and execution of various cryptographic tasks using the unique capabilities and power of quantum computers. Theoretically, this type of computer can aid the development of new, stronger, more efficient encryption systems that are impossible using existing, traditional computing and communication architectures. While many areas of this science are conceptual rather than a reality today, several important applications where encryption systems intersect with quantum computing are essential to the immediate future of cybersecurity. Two popular, yet distinctly different cryptographic applications that are under development using quantum properties include:
Quantum-safe cryptography: The development of cryptographic algorithms, also known as PoST-quantum cryptography, that are secure against an attack by a quantum computer and used in generating quantum-safe certificates.
Quantum key distribution: The process of using quantum communication to establish a shared key between two trusted parties so that an untrusted eavesdropper cannot learn anything about that key.

a) Use Cases

- Encryption and authentication of endpoint devices

Endpoint devices include any piece of hardware that a user utilizes to interact with a distributed
computing system or network. This can include canonical examples such as personal computers and mobile phones, as well as kiosks/terminals in banks, stores, and airports, as well as any kind of embedded technology connected to a broader network. Encryption of endpoint devices refers to the practice of making the contents of the device unreadable to unauthorized parties through the use of cryptography and security protocols. This is an important practice to prevent unauthorized data transfer and access, to ensure that only approved devices are allowed access to the system, and to deal appropriately with rogue or compromised devices that threaten system security through intrusions such as malware, key loggers, or viruses.

- Cloud Storage and computing

Options for quantum-safe cloud computing are subsumed by quantum-safe server, endpoint, and network infrastructure security. Key exchange parameters for protocols such as HTTPS should no longer make use of RSA, DSA, or ECDSA. Fortunately, cloud computing offers the distinct advantage of having a centralized IT security management system across many applications and businesses, reducing security overhead for individual enterprises and consequently offering easier transition to quantum-safe protocols. This transition is essential in particular due to both the fact that cloud storage is – by definition – remotely accessed, requiring data to traverse a public network between the user and the cloud. The need for strong encryption is further amplified by the multitude of distinct and untrusted users sharing the infrastructure.

b) Fields of application

- Medicine and health

Medicine and health services in industrialized countries share core values of patient confidentiality, which is increasingly important giving the rising ubiquity of regional and national public health information networks, as well as multi-clinic information systems for centralized patient records.

- Financial Services

Banks and financial services rely heavily on information technology in their operations, and as a consequence are extensive users of cryptography to guarantee authenticity, integrity and confidentiality of the information they process.

- Mobile Applications

Mobile applications may or may not be owned and controlled by a Mobile Network Operator (MNO), the availability of these applications and services are often a deciding factor for users as to which handset they will purchase and to which mobile network they will subscribe.

- Mobile Network Operator Wholesale

Internet of Things - M2M, sensors are used everywhere to remotely monitor assets and communicate back to their owners. Electrical meters, vending machines, shipping containers, medical monitoring equipment are some of the examples of embedded devices that require remote connectivity that either uses a proprietary dedicated wireless network or purchases wireless cellular bandwidth from an MNO as a wholesale application. Many commercial applications have regulated security requirements, often with unique and constrained cryptographic key management needs.
Connected Vehicles, telematics and emerging vehicle-to-vehicle communications used for fleet logistics and public safety applications. Many of these applications rely on confidential and authentic communications

D. Blockchain Technology

Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the “chain,” in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a ‘digital ledger. ‘Every transaction in this ledger is authorized by the digital signature of the owner, which authenticates the transaction and safeguards it from tampering. Hence, the information the digital ledger contains is highly secure.

Security is not the only benefit of blockchain technology. Blockchain technology makes sure the owner of the data is anonymous. All the sensitive information about identity is protected. Whenever a user tries to obtain the data, all the sections are validated to check for alterations. If any alteration is found, the miner responsible for that is eliminated from the network. From big tech corporations to entrepreneurs, several companies have jumped to the blockchain cloud storage market, transforming their businesses digitally. Blockchain provides not only secure but also a cheap way to get cloud storage because many small organizations collaborate to share the computing power and space to store data. This way, cloud storage costs are reduced, and organizations that chip in computing power also get paid.

1) History of Blockchain

Satoshi Nakamoto, whose real identity still remains unknown to date, first introduced the concept of blockchains in 2008. The design continued to improve and evolve, with Nakamoto using a Hash cash-like method. It eventually became a primary component of bitcoin, a popular form of cryptocurrency, where it serves as a public ledger for all network transactions. Bitcoin blockchain file sizes, which contained all transactions and records on the network, continued to grow substantially. By August 2014, it had reached 20 gigabytes, and eventually exceeded 200 gigabytes by early 2020.

2) Key elements of a blockchain

- Distributed ledger technology

All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.

- Immutable records

No participant can change or tamper with a transaction after it's been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.

- Smart contracts

To speed transactions, a set of rules — called a smart contract — is stored on the blockchain and executed automatically. A smart contract can define conditions for corporate bond transfers, include terms for travel insurance to be paid and much more.

3) Types of Blockchain

All types of blockchains can be characterized as permissionless, permissioned, or both. Permissionless blockchains allow any user to pseudo-anonymously join the blockchain network (that is, to become "nodes" of the network) and do not restrict the rights of the nodes on the blockchain network. Conversely, permissioned blockchains restrict access to the network to certain nodes and may also restrict the rights of those nodes on that network. The identities of the users of a permissioned blockchain are known to the other users of that permissioned blockchain. Blockchain Buzzwords Permissionless blockchains tend to be more secure than permissioned blockchains, because there are many nodes to validate transactions, and it would be difficult for bad actors to collude on the network.

Three types of blockchain

- Public blockchain.

A public, or permission-less, blockchain network is one where anyone can participate without restrictions. Most types of cryptocurrencies run on a public blockchain that is governed by rules or consensus algorithms.

- Permissioned or private blockchain.

A private, or permissioned, blockchain allows organizations to set controls on who can access blockchain data. Only users who are granted permissions can access specific sets of data. Oracle Blockchain Platform is a permissioned blockchain.

- Federated or consortium blockchain.

A blockchain network where the consensus process (mining process) is closely controlled by a preselected set of nodes or by a preselected number of stakeholders.

4) Benefits of blockchain

- Greater trust

With blockchain, as a member of a members-only network, you can rest assured that you are receiving accurate and timely data, and that your confidential blockchain records will be shared only with network members to whom you have specifically granted access.

- Greater security

Consensus on data accuracy is required from all network members, and all validated transactions are immutable because they are recorded permanently. No one, not even a system administrator, can delete a transaction.

- More efficiencies

With a distributed ledger that is shared among members of a network, time-wasting record reconciliations are eliminated. And to speed transactions, a set of rules — called a smart contract — can be stored on the blockchain and executed automatically.

5) Top blockchain use cases for cybersecurity

Due to its nature, the blockchain offers promising cybersecurity options to startups and enterprises operating in different fields. The list of sectors that can benefit the most from applying the blockchain for cybersecurity includes.

E. Objective of the Project

The objective of the project is to manage data and authority, a decentralized personal data management system can be achieved by introducing blockchain technology into the satellite communication network and combining blockchain technology with an off-chain database to separate data and data authority.

II. SYSTEM ANALYSIS

A. Existing System

Satellite Communication comes with many benefits and various risks. Cryptographic algorithms should develop security solutions that protect GEO Satellite networks and minimize security risks. As security is the prime concern for any communications, the traditional security techniques are

- AES

AES Rijndael's proposal for AES (Advanced Encryption Standard) uses 128, 192, and 256 bits to decode a number that allows the block length and key length to be specified independently of each other. The key length determines some parameters of the AES algorithm.

- DES

DES (Standard Encryption Standard) is a 64-bit symmetric block encryption algorithm. This algorithm works on 64-bit blocks of plain text. Due to the symmetry, the same key can be used for encryption and decryption. In most cases, the same algorithm is used for encryption and decryption. First, the transition is performed according to a fixed table (initial permutation), which divides a 64-bit block of plain text into two 32-bit blocks, each of which performs 16 identical operations, called rounds. The two halves are connected, and the first inversion of the permutation is performed. The purpose of the first implementation is clear. This does not affect the security of the algorithm. Therefore, small blocks of plain text and cipher text can be loaded into an 8-bit chip. Only half of the original 64-bit block is used in one run. The rounds alternate between the two halves.

- Triple-DES

Triple-DES is a type of computer encryption algorithm in which each data block receives three passes. Triple DES is currently considered obsolete, but some IoT products use it for compatibility and flexibility. Triple DES is a good encryption algorithm that can be used to protect against brute force attacks. "Brute force" is a painstaking effort (as opposed to an intelligent strategy) through repeated attempts and efforts. The Brute Force attack automatically uses automated tools and then it therefore it takes guesses various combinations until a hacker breaks the key.

- Blowfish

Blowfish is a block cipher and is a part of symmetric key encryption. It encrypts data in blocks of 8 bytes. The algorithm consists of two parts, a key extension part and a data encryption part. The key extension converts a key with a maximum length of 56 bytes (448 bits) into several tables with subkeys with a total of 4168 bytes.

- Hash functions.

New cryptographic hash algorithm “SHA-3” competition attracts many people’s attention. SHA-3 is expected to be a general-purpose hash function, and none of the current finalists do not satisfy lightweight properties. Research on lightweight dedicated hash functions has been just started. They are too immature to adopt now. It is possible to construct lightweight hash functions based on lightweight block ciphers.

- Elliptic curve cryptography (ECC)

It is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

- Private key authentication

Private key cryptography is asymmetric encryption which provides two keys, one public and one private. If data are encrypted with the private key, it can only be decrypted with the public key, and vice versa. Doing so preserves the security of the system and makes communications with other devices safer. This can be useful when a new device needs to connect to the IoT network and in the verification of messages passed between devices.

- Signed firmware

While creating the firmware, the developer puts a secret digital signature with it, preventing hackers from replacing the actual firmware with a malicious one as they will not be able to replicate authenticated signatures. Also, a technique called secure boot is used to check if each code that runs on the device is signed appropriately.

All these techniques mentioned above are not realizable to a very good extent in real-life systems due to resource constraints. A restricted amount of processing power and memory poses a big hurdle for developers. These techniques may be theoretically perfect but there are various different examples where we can still see security breaches in IoT systems.

1) Disadvantages

- Encryption methodologies are becoming less reliable as the eavesdroppers and attackers are gaining powerful computing ability.
- Many of these solutions employ static authentication, which verifies the user/device just once at the beginning of each session.
- Does not prevent man-in-the middle attack and fails to prevent a collision attack.
- Does not provide backward and forward secrecy as the attacker can gain the ID of the devices, then sniff other values from the current session to find the previous and future secret keys.
- Does not provide anonymity and untrace ability.
- Initialization and computation cost high.

B. Proposed System

There are essentially three types of orbits classified by the satellite altitude: geostationary earth orbit (GEO), medium earth orbit (MEO), and low earth orbit (LEO). Among them, GEO satellites are stationary relative to the earth’s surface so that the doppler shift is negligible and has a lower transmission outage probability than non-GEO satellites. The GEO satellites work at very high altitudes (≈35,786 km) and can offer the most extensive coverage. Thanks to the low outage probability and wide coverage, GEO satellites are preferred in our proposed protocol.

Satellite communications systems enable the sending and receiving of information worldwide, offering internet access, television, telephone, radio, and other civilian and military operations. The advent of HIS (high-throughput satellite) systems has greatly enhanced technical capabilities and offered wideband services at lower costs. Significant improvements are expected on the forthcoming mega-constellations in low Earth orbits that willed play thousands of satellites, providing full earth coverage to minimize delays in addition to wide bandwidth. The use of satellites, given these characteristics, can increase efficiency in providing large sets of services and applications that are security-sensitive, such as telemedicine, banking, search and rescue, sensor networks, and content delivery network feed. However, in many cases, the security of satellite

communication has been seriously compromised, resulting in covert dangers. In satellite communications (and even in terrestrial systems), hackers can interfere, intercept, or modify wireless network systems remotely, attack the equipment of flight crews, and control the positioning and transmission of satellite communication antennas. According to satellite communication protocols, the use of space in satellite communications can be developed independently to enhance communication security. Recommendations have been proposed to further increase the unity and compatibility of communication protocols for space. A single security mechanism is insufficient to meet the security requirements for satellite communication services. In this project, Quantum Key Cryptography and block chain technology is introduced to analyse the security of satellite communication networks in terms of access control, confidentiality, and security authentication.

1) Quantum Cryptography

Quantum cryptography, also called quantum encryption, applies principles of quantum mechanics to encrypt messages in a way that it is never read by anyone outside of the intended recipient. It takes advantage of quantum's multiple states, coupled with its "no change theory," which means it cannot be unknowingly interrupted.

- Quantum-safe cryptography:

The development of cryptographic algorithms, also known as PoST-quantum cryptography, that are secure against an attack by a quantum computer and used in generating quantum-safe certificates. Quantum cryptography uses the same physics principles and similar technology to communicate over a dedicated communications link. The goal of PoST-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.

PoST Quantum Cryptography

PQC links private keys to public keys without using problems that quantum computers can easily solve. In other words, it aims to deliver the benefits of today's public-key encryption without the vulnerability to quantum hacking.

Approaches to PQC include building encryption around mathematical "structures" called lattices, using systems purely based upon code, solving complicated problems involving multiple variables, and much more.

- Quantum key distribution:

The process of using quantum communication to establish a shared key between two trusted parties so that an untrusted eavesdropper cannot learn anything about that key. Quantum key distribution utilizes the unique properties of quantum mechanical systems to generate and distribute cryptographic keying material using special purpose technology.

Quantum Key Generation: Internet key exchange version 2 (IKEv2) Internet Key Exchange (IKEv2) is a protocol used to establish keys and security associations (SAs) for the purpose of setting up a secure Satellite Network (SN) connection that protects data packets from being read or intercepted over a public Internet connection. This allows a remote computer on a public network to access resources and benefit from the security of a private closed network without compromising security. The IKE protocol standard is rigid and does not permit SN designers to choose beyond a small set of cryptographic algorithms. The shared secrets provided by QKD may either be used with conventional encryption ciphers, or for one-time pad encryption in high security applications' may also be used for the second pass to solve the key management problem of distributing shared secret keys for message authentication. Instead of calculating shared secrets and computing secret keys, QKD keys could be used to protect integrity

IKE also provides authenticated connections, using RSA, DSS or MAC with a pre-shared secret. While the MAC option with proper key and MAC tag length justification is quantum safe, RSA and DSS algorithms are not. Simply specifying the use of a MAC with pre-shared secret is not an adequate substitute for a public key-based algorithms because a large network with individual pre shared secrets for every connection does not scale well and quickly becomes a key management problem as the network grows. Pre-shared keys are also problematic in a large network because, if a global key is being used it is very hard to keep such a global key a secret, representing a vulnerability with a single point of failure.

Internet Protocol Security (IP Sec) encryption has been the standard used to secure data any time it moves between two or more classical computers and/or networks over the internet. It includes existing communications protocols for establishing mutual authentication between agents at the beginning of a session, and negotiation of cryptographic keys to use during the session.

Internet Key Exchange (IKE) is the protocol used to set up a security association in the IP Sec protocol suite, and it comes in two flavors, IKEv1 and IKEv2.IKEv2 is based on the Diffie-Hellman (DH) exchange, created to allow two parties to jointly establish a shared secret cryptographic key over an insecure public channel. Today, all of the authentication methods that make IKEv2 possible can be broken by a large-scale quantum computer. Common methods for establishing authentication over IKEv2 include RSA and Elliptic Curve Digital Signature Algorithms (ECDSA).By contrast, IKEv1 does not rely just on a DH exchange to establish authentication. Initially, IKEv1 was meant for more general-purpose key exchange, and thus had many extraneous features that were removed with the switch to IKEv2.

2) SatChain

A consortium blockchain is introduced for sharing information among cooperative satellite constellations. In this section, a new concept, called Sat Chain, is proposed. SatChain's are a way to tokenize space transactions as digital tokens that can be processed using a blockchain protocol to authenticate space transactions. SDTs can be broadcast within a swarm of satellite networks called a satellite constellation. Hence, blockchain can work in this scenario as an authenticator for all communication patterns that can occur within a specific satellite's constellation. SatChain's are used to process sensing data between satellites and DPC; hence, blockchain can work in this scenario as a tracking system to detect expected space collisions between satellites and DPC

Satellite network or sensing data between a satellite and DCP. The blockchain protocol is responsible for verifying

the new space transactions to add a new valid block to the blockchain. All space stakeholders are then able to access the newly added blocks through the connected dashboard to the blockchain platform that manages a satellite constellation. Each space transaction has to be converted into a Satellite Encrypted Data (SED) or Space Digital Tokens (SDT)). This new transaction (i.e., SED) has to be verified using a blockchain protocol (or consensus) to confirm the validation of a specific transaction between two satellites in the same constellation. Additionally, the blockchain protocol is responsible for validating all transactions exchanged within a satellite constellation. If the handled SED is valid, anew block is added to the blockchain. The new block contains all details of the new space transaction. This new information can be used by space stakeholders who are authorized to access the blockchain.

3) Proof of Space Transactions (POST)

Proof of Space Transactions (POST) is a novel blockchain protocol that can be utilized to verify SEDs within a satellite's constellation and to add a new block to the blockchain. The POST methodology represents each satellite within a constellation as a private key and a piece of cryptographic evidence for a satellite's private key that is cryptographically attached to a specific SED. When a new SED is triggered between two satellites, the satellite that created the transaction shares the cryptographic evidence of this transaction with the rest of the satellite constellation to confirm the validity of the triggered SED. In addition, the receiving satellite requests the nonce code of the last block of the blockchain. Once the nonce code is confirmed by the receiving satellite, a new block is added to the blockchain.

4) Advantages

- The ability to make secured communications with a satellite through an untrusted ground station.
- The ability to have separate channels of communication while keeping as many points of contact to satellites as possible.
- Immutable, non-repudiable, distributed record of commands and communications
- Automation of satellite observations
- Automatic routing of commands to any ground stations with line of sight to satellites
- Downlink satellites data at any ground station and automatically distributed to all desired parties
- Pass secured, encrypted data through unsecured ground stations
- Fine-grained access control over distributed data
- Data Integrity in GS network
- Fraud protection in the resulting transactions ledger
- Centralized certificate authority or cross-certification methods not needed
- Data Distribution System network, being distributed, is far less exposed to malicious attacks
- Smart contracts are digitally signed so they cannot be tampered.

III. SYSTEM DESIGN

A. System Flow

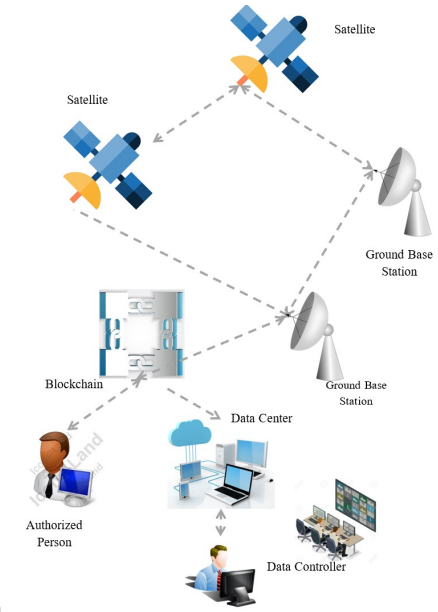

Fig. 3.1. System flow

B. System Architecture

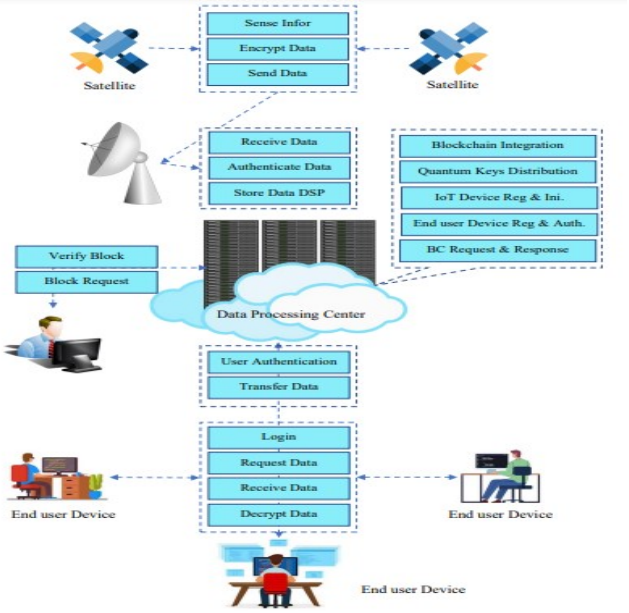

Fig. 3.2. System Architecture

IV. PROJECT DESCRIPTION

A. Problem Definition

The implementation phase will involve the development and testing of the proposed solution in a laboratory environment. This phase will include the setup and configuration of the QKD and blockchain systems, as well as the implementation of the communication protocol. The methodology of the project will be described, including the steps involved in designing and implementing the proposed solution, evaluating its performance, validating it through real-world testing, and discussing the findings.

The system implementation for secure satellite communication using quantum PKI for external threat and blockchain for internal threat in a satellite data processing center involves the following steps:

- Set up a satellite network using Tkinter or PHP and MySQL for the satellite data processing centre.
- Implement quantum cryptography to establish secure communication between the satellite and ground station.
- Develop a blockchain-based system to prevent insider attacks in the satellite data processing centre.
- Implement the system using Python for the satellite with Tkinter and PHP for the satellite data processing canter with MySQL database.

The following are the detailed steps for each component of the system:

- Satellite Network Setup:

For the satellite, a Tkinter-based GUI can be developed to simulate the satellite network. The GUI can have options for establishing communication with the ground station, transmitting data, and receiving data from the ground station. For the satellite data processing canter, a PHP-based web interface can be developed to manage data received from the satellite. A MySQL database can be used to store the data.

- Quantum Cryptography Implementation:

Implement quantum key distribution (QKD) to establish secure communication between the satellite and ground station. This can be done using a software-based QKD simulator or by using physical quantum hardware. Once the quantum keys are exchanged, they can be used to encrypt and decrypt the data transmitted between the satellite and ground station.

- Blockchain-based System for Insider Attack Prevention:

Develop a blockchain-based system to prevent insider attacks in the satellite data processing centre. The system can be designed to allow only authorized personnel to access the data and perform specific operations. The blockchain can be used to maintain an immutable record of all transactions and changes made to the data. The system can also be designed to automatically detect and flag any suspicious activity, such as unauthorized access or modification of data.

- System Implementation:

Implement the system using Python for the satellite with Tkinter and PHP for the satellite data processing center with MySQL database. The satellite can be programmed to encrypt and transmit the data to the ground station using the quantum keys. The ground station can be programmed to receive the encrypted data, decrypt it using the quantum keys, and store it in the MySQL database. The blockchain-based system can be implemented in PHP and integrated with the MySQL database to prevent insider attacks in the satellite data processing center. Thus, the system implementation involves developing a satellite network, implementing quantum cryptography for secure communication, developing a blockchain-based system for insider attack prevention, and integrating these components to create a secure and reliable satellite communication system.

B. Modules Description

1) Data Processing Center Server App

Fig.4.1 shows that the Satellite network system structure model in this project is composed of a Satellite, Ground Station, Data Processing Center, Satellite Controller or Operator through a lightweight wireless network connection. Each satellite connects to GS. The following describes the functions and permissions of each section:

DPC layer comprises one or many servers. These servers support other layers for the registration of devices and the establishment of a secure communication. Additionally, it allows end users to register and communicate with the system. The system is responsible for preparing the satellite mission plan and completing the transmission management for the user station responsible for satellite monitoring. This system is also responsible for receiving, processing and distributing user station data.

a) Registration and Initialization Phase

End User and Device Registration: users can be humans or any digital device, application, service, or software agent that interacts indirectly or directly with the physical entity or the system. Here two types of End users

- Default Users
  - i) Trusted Authority
  - ii) DPC Admin
- Customized User
  - iii) Satellite
  - iv) Ground Station
  - v) Satellite Controller or Operator
  - vi) Satellite Operator Device

2) Quantum Key Generation and Distribution

Key Gen Satellite Operator (SO1): To register Satellite Operator, DPCA selects an identity Satellite Operator Device Unique Features and distribute to Quantum RSA-based private-public key pairs ($r_{BBA} \in Z^*_q$, $Pub_{BBA} = r_{BBA} \cdot G$).

Key Gen Satellite (SAT1): DPCA picks a unique identity IDα, a unique master key MKα, and Quantum RSA-based private-public key pairs ($r_\alpha \in Z^*_q$, $Pub_{SATV\alpha} = r_\alpha \cdot G$) for each Satellite, SAT_α, where $\{\alpha = 1, 2, \cdots, n\}$ and n is the total number of SAT to be registered.

a) PoST Quantum Cryptography

- ENCRYPTION

  When satellite i sends a message, it uses its private key and the signature key certification parameters received from the DPC in order to sign the message. The signature assures receivers that the message was sent by an authenticated member of the group and was not changed during transmission. In order to sign the message, the vehicle first chooses a random number $b \in Z^*p$ and generates a timestamp T. M is the message to sign.

After generating the signature, vehicle i broadcasts message M along with σ M, PKi, T, A, and B.

- DECRYPTION

  Any receiver of the message who wishes to validate it first checks the timestamp. If $T_{now} - T > T_{replay}$ then the message will be discarded as a potential replay attack.

3) SatChain Integration

A consortium blockchain is introduced for sharing information among cooperative satellite constellations. In this section, a new concept, called SatChain, is proposed. SatChain's are a way to tokenize space transactions as digital tokens that can be processed using a blockchain protocol to authenticate space transactions. SDTs can be broadcast within a swarm of satellite networks called a satellite constellation. Hence, blockchain can work in this scenario as an authenticator for all communication patterns that can occur within a specific satellite's constellation. SatChain's are used to process sensing data between satellites and DPC; hence, blockchain can work in this scenario as a tracking system to detect expected space collisions between satellites and DPC.

Satellite network or sensing data between a satellite and DCP. The blockchain protocol is responsible for verifying the new space transactions to add a new valid block to the blockchain. All space stakeholders are then able to access the newly added blocks through the connected dashboard to the blockchain platform that manages a satellite constellation. Each space transaction has to be converted into a Satellite Encrypted Data (SED) or Space Digital Tokens (SDT)). This new transaction (i.e., SED) has to be verified using a blockchain protocol (or consensus) to confirm the validation of a specific transaction between two satellites in the same constellation. Additionally, the blockchain protocol is responsible for validating all transactions exchanged within a satellite constellation. If the handled SED is valid, anew block is added to the blockchain. The new block contains all details of the new space transaction. This new information can be used by space stakeholders who are authorized to access the blockchain.

a) Proof of Space Transactions (PoST)

Proof of Space Transactions (PoST) is a novel blockchain protocol that can be utilized to verify SEDs within a satellite's constellation and to add a new block to the blockchain. The PoST methodology represents each satellite within a constellation as a private key and a piece of cryptographic evidence for a satellite's private key that is cryptographically attached to a specific SED. When a new SED is triggered between two satellites, the satellite that created the transaction shares the cryptographic evidence of this transaction with the rest of the satellite constellation to confirm the validity of the triggered SED. In addition, the receiving satellite requests the nonce code of the last block of the blockchain. Once the nonce code is confirmed by the receiving satellite, a new block is added to the blockchain

V. CONCLUSION

The satellite communication channel is different not only from the common mobile channel but also from the ground station channel. The satellite communication channel is the fusion of the satellite channel and the mobile communication channel. Satellite communication channels are extremely vulnerable to hackers and external interference signals. Protecting satellite networks from illegal information access and use can be extremely challenging. In this project, Quantum Key Cryptography and blockchain technology is introduced to analyze the security of satellite communication networks in terms of access control, confidentiality, and security authentication. The proposed scheme is developed to solve the security problem of using a centralized database in satellite communication. The simulation results show that the proposed method was able to significantly improve security and protection for satellite communications.

VI. REFERENCES

[1] S. Fu, J. Gao, and L. Zhao, ``Integrated resource management for terrestrial-satellite systems," IEEE Trans. Veh. Technol., vol. 69, no. 3, pp. 3256-3266, Mar. 2020.

[2] Christo Ananth , P.Ebenezer Benjamin, S.Abishek, "Traffic Light Based Intelligent Routing Strategy for Satellite Network", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Special Issue 2 - November 2015, pp.24-27.

[3] Christo Ananth, D.L.Roshni Bai, K.Renuka, A.Vidhya, C.Savithra, "Liver And Hepatic Tumors Segmentation in 3-D CT Images", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3,Issue-2, February 2014,pp 496-503

[4] C. Li, L. Zhu, Z. Luo, and Z. Zhang, ``Solutions to data reception with improve blind source separation in satellite communications,'' in Proc. IEEE Int. Symp. Netw., Comput. Commun. (ISNCC), Montreal, QC, Canada, Oct. 2020, pp. 1-5.