BLOCK CHAIN BASED CYBER SECURITY SYSTEM FOR DATA TRANSFER

BOBBY K SIMON, ANJANA P NAIR

[1]BOBBY K SIMON, M.Tech Computer Science & Engineering. Sree Buddha College of Engineering, Ayathil, Elavumthitta Pathanamthitta, Kerala, India.
[2]S Ms. ANJANA P NAIR, Assistant Professor Computer Science & Engineering. Sree Buddha College of Engineering, Ayathil, Elavumthitta, Pathanamthitta, Kerala, India

Abstract - *GPRS terminals are utilized as inward or outside specialized gadgets, sending charge related data from financial money registers and monetary printers to an expense organization server, so cyber security is of fundamental significance. This paper examines cyber security of GPRS terminals, which are utilized in numerous nations. With a huge amount of personal data in big data era, fiscal devices are at high risks associated with potential disclosure of privacy data. Fiscal devices should overcome various types of threads including viruses, malicious apps, and spam. In this paper, we propose trustworthy, reducing the storage space and protect the data transfer, n which communication information copies are encrypted to distribute and reducing the storage size after block chain validation.*

Key Words: **FISCAL DEVICE, BLOCKCHAIN, SMART CONTACT, DLT, GPRS.**

1. INTRODUCTION

Data is becoming one of the most valuable resources in the world. The list of the top 10 companies by market capitalization is now dominated by data-centric companies like Facebook, Alphabet, Microsoft, Apple, and Amazon. That value means your data, especially your sensitive data, is now a prime target for cyber criminals, and you probably aren't as protected as you think. Inventory network use cases are the most widely recognized utilization of blockchain for tackling genuine business or banking data issues because of the absence of precisviblity of transfer information for item or part data as the travels through the production[4] network. Transfer delays are frequently because of middle people inside the inventory network whose job is endorsement of desk work related with the confidential data. Administrative work tends to get lost or lost, or is anticipating handling as the heaps of desk work develop. Imagine a scenario where this desk work could be digitized on the blockchain. The requirement for these sorts of delegates could be expelled from the production network.

The blockchain would catch key transfer information discharged from fiscal gadgets appended to items or on the other hand segments as the transfer moves from source to goal. The IoT stage would conjure an exchange for the blockchain that contains the transfer compartment area and time stamp. The exchanges caught in the blockchain would fill in as evidence of transfer and evidence of conveyance for holder data transfer. Transfer postponements would be limited and lead times for data streaming to assembling offices could be all the more precisely anticipated. If you have been following banking, investing, or data transferring over the last ten years, you may be familiar with "blockchain," the record-keeping technology behind bitcoin. And there's a good chance that it only makes so much sense. In trying to learn more about block chain, you've probably encountered a definition like this: "blockchain is a distributed, decentralized, public ledger." The good news is, block chain is actually easier to understand than that definition sounds.

Data levels at the offices could be better lined up with in the nick of time rehearses. Block chain technology enables distributed public ledgers that hold immutable data in a secure and encrypted way and ensure that transactions can never be altered. While data and other crypto currencies are the most popular examples of block chain usage, this "distributed ledger technology" (DLT) is finding a broad range of uses. Data storage, financial transactions, real estate, asset management and many more uses are being explored.

2. RELATED WORK

2.1 What is Blockchain, Really?

If this technology is so complex, why call it "blockchain?" At its most basic level, blockchain is literally just a chain of blocks, but not in the traditional sense of those words. When we say the words "block" and "chain" in this context, we are actually talking about digital information (the "block") [2] stored in a public database (the "chain").

Blockchain technology has been one of the major technological breakthroughs of this century. Bitcoin, the first Blockchain application, allows a network of users to perform transactions without requiring the trust of anyone on the network, or a third party. Everything is encrypted, and nobody can tamper with the Blockchain without everyone else noticing immediately. Bitcoin has deeply penetrated into our daily lives and proven to be remarkably effective as an investment, means of payment and earning asset. Today the cryptocurrency ecosystem is advanced enough to let practically everybody get into Bitcoin at the click of a button. There are cryptocurrency exchanges like that provide users with a wide range of tools for trading, buying and selling, as well as simply storing Bitcoins and altcoins[7] securely on their platforms.

"Blocks" on the blockchain are made up of digital pieces of information. Specifically, they have three parts:

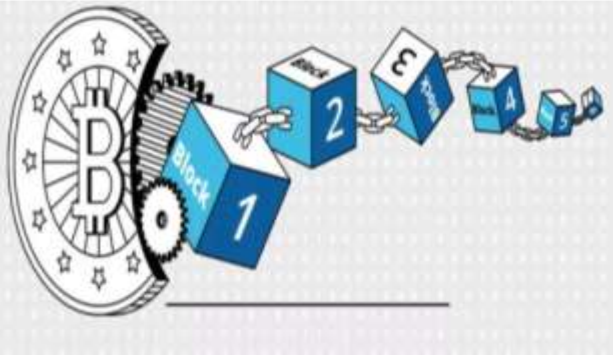

Fig -1: Bitcoin based blockchain.

2.2 How Does Blockchain Work?

When a block stores new data it is added to the blockchain. Blockchain, as its name suggests, consists of multiple blocks strung together. In order for a block to be added to the blockchain, however, four things must happen:

i. A transaction must occur. Let's continue with the example of your impulsive Amazon purchase. After hastily clicking through multiple checkout prompts, you go against your better judgment and make a purchase.

ii. That transaction must be verified. After making that purchase, your transaction must be verified. With other public records of information, like the Securities Exchange Commission, Wikipedia, or your local library, there's someone in charge of vetting new data entries. With blockchain, however, that job is left up to a network of computers. These networks often consist of thousands (or in the case of Bitcoin, about 5 million) computers spread across the globe. When you make your purchase from Amazon, that network of computers rushes to check that your transaction happened in the way you said it did. That is, they confirm the details of the purchase, including the transaction's time, dollar amount, and participants. (More on how this happens in a second.)

iii. That transaction must be stored in a block. After your transaction has been verified as accurate, it gets the green light. The transaction's dollar amount, your digital signature, and Amazon's digital signature are all stored in a block. There, the transaction will likely join hundreds, or thousands, of others like it.

iv. That block must be given a hash. Not unlike an angel earning its wings, once all of a block's transactions have been verified, it must be given a unique, identifying code called a hash. The block is also given the hash of the most recent block added to the blockchain. Once hashed, the block can be added to the blockchain.

When that new block is added to the blockchain, it becomes publicly available for anyone to view — even you. If you take a look at data's blockchain, you will see that you have access to transaction data, along with information about when ("Time"), where ("Height"), and by who ("Relayed By")[1] the block was added to the blockchain. Anyone can view the contents of the blockchain, but users can also opt to connect their computers to the blockchain network. In doing so, their computer receives a copy of the blockchain that is updated automatically whenever a new block is added, sort of like a facebook[5] News Feed that live updates whenever a new status is posted.

Each computer in the blockchain network has its own copy of the blockchain, which means that there are thousands, or in the case of Bitcoin, millions of copies of the same blockchain. Although each copy of the blockchain is identical, spreading that information across a network of computers makes the information more difficult to manipulate. With blockchain, there isn't a single, definitive account of events that can be manipulated. Instead, a hacker would need to manipulate every copy of the blockchain on the network.

Looking over the Bitcoin blockchain, however, you will notice that you do not have access to identifying information about the users making transactions. Although transactions on blockchain are not completely anonymous, personal information about users is limited to their digital signature, or username.

2.3. How does blockchain improve data security?

In the realm of data security, it could prove transformative, but it's not a panacea. If you're considering adopting it, then take some time to understand it and how it can help your business first. You need a clear strategy [3]and solid reasons to adopt a new technology, no matter how much buzz it's generating. Let's take a closer look at four ways blockchain could have a positive impact on data security. Heralded as a major disruptor for countless industries, there's no doubt that blockchain offers some important potential advantages for the business world. Instead of uploading data to a cloud server or storing it in a single location, blockchain breaks everything into small chunks and distributes them across the entire network of computers. It's a digital ledger of transactions that lacks a central control point. Each computer, or node, has a complete copy of the ledger, so one or two nodes going down will not result in any data loss[6].

2.3.1. Blockchain is virtually impossible to hack

While hackers can break into traditional networks and find all the data in a single repository and exfiltrate it or corrupt it, the blockchain makes this unfeasibly hard. The data is decentralized, encrypted, and cross-checked by the whole network. Once a record is on the ledger it's almost impossible to alter or remove without it being noticed and invalidating the signature.

It effectively cuts out the middle man – there is no need to engage a third-party to process a transaction. You don't have to place your trust in a vendor or service provider when you can rely on a decentralized, immutable ledger. Blockchain offers encryption and validation. Everything that occurs on the blockchain is encrypted and it's possible to prove that data has not been altered. Because of its distributed nature, you can check file signatures across all the ledgers on all the nodes in the network and verify that they haven't been changed. If someone does change a record, then the signature is rendered invalid. This potentially allows you to use the blockchain ledger to verify that data you backed up and stored in the cloud with third-party vendors has gone completely unchanged even weeks, months, or years later. Nobody can deny that blockchain offers reliable, independent data verification.

Every legitimate transaction is confirmed by multiple nodes on the network. To successfully hack blockchain, you would have to hack most of the nodes simultaneously, which, though technically possible with enough supercomputing power and time, is well beyond the ability of cybercriminals today.

2.3.2 All blockchains are not created equal

It is important to be aware of this fact when evaluating whether the technology you've chosen will have the security you require. Today, there are two main types of blockchain, public and private, with a number of variations. Public and private blockchains differ in a couple of key ways that can affect the level of security they provide.

The most obvious difference is that public blockchains use computers connected to the public internet to validate transactions and bundle them into blocks to add to the ledger. Any computer connected to the internet can join the party. Private blockchains, on the other hand, typically only permit known organizations to join. Together, they form a private, members-only "business network." This difference has significant implications in terms of where the (potentially confidential) information moving through the network is stored and who has access to it. Just from that, you can probably see how a public blockchain might not be right for enterprise. Another important and related difference is that public blockchains are typically designed around the principle of anonymity, whereas private blockchains use identity to confirm membership and access privileges, and so the participants in the network know exactly who they are dealing with.

The other main way public and private blockchains differ is how transactions are verified. Basically, for a transaction to be added to a blockchain, network participants must agree that it is the one and only version of the truth. That is done through consensus, which means *agreement*. Bitcoin is probably the most well-known example of a public blockchain and it achieves consensus through "mining." In Bitcoin mining, computers on the network (or 'miners') try to solve a complex cryptographic problem to create a proof of work. The drawback is that this requires an enormous amount of computational power, especially for large-scale public blockchains.

Alternatively, a private blockchain consists of a permission network in which consensus can be achieved through a process called "selective endorsement," where known users verify the transactions. The advantage of this for businesses is that only participants with the appropriate access and permissions can maintain the transaction ledger. There are still a few issues with this method, including threats from insiders, but many of them can be solved with a highly secure infrastructure.

When establishing a private blockchain, you must decide the best platform for deployment. Even though blockchain has inherent properties that provide security, known vulnerabilities in your infrastructure can be manipulated by those with ill intent. Ideally, you should have an infrastructure with integrated security that can:

i. Prevent anyone — even root users and administrators from accessing sensitive information

ii. Deny illicit attempts to change data or applications within the network.

iii. Carefully guard encryption keys using the highest-grade security standards so they can never be misappropriated.

With these capabilities, your blockchain network will have the added protection it needs to prevent attacks from within and without. To learn more about the only fully integrated enterprise-ready blockchain platform designed to accelerate the development, governance and operation of a multi-institution business network.

2.4 Data storage in Blockchain

Ordinary people can now rent out part of their unused hard drive space and earn money for doing so. The ability to leverage excess storage capacity has become a reality thanks to the incentives being offered by various companies that are seeking to expand their decentralized networks.

Blockchain Data Storage: This technology will be used to create new, decentralized data storage networks, putting the power of choice back in the end-user's hands. One of the most heralded achievements of the internet era, both for personal and industry use, is cloud data storage.

A blockchain-based storage system prepares the data for storage and then distributes it across a decentralized infrastructure, a process that can be broken into the six steps that follow:

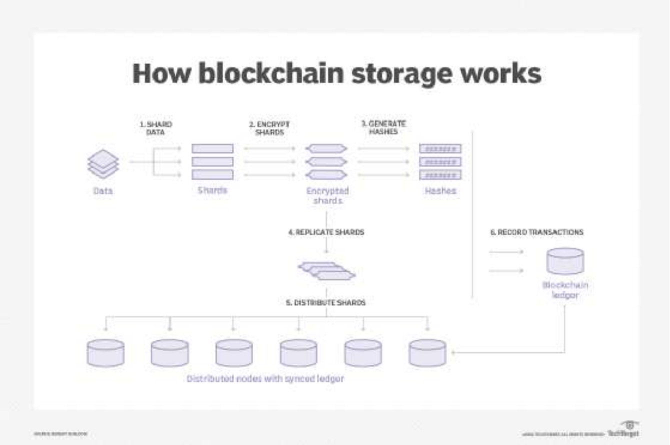

Fig -2: Data can store in blockchain

i. Create data shards:- The storage system breaks the data into smaller segments, a process called sharding. Sharding involves breaking the data into manageable chunks that can be distributed across multiple nodes. The exact approach to sharding depends on the type of data and the application doing the sharding. Sharding a relational database is different from sharding a NoSQL database or sharding files on a file share.

ii. Encrypt each shard: - The storage system then encrypts each data shard on the local system. The content owner has complete control over this process. The goal is to ensure that no one other than the content owner can view or access the data in a shard, wherever the data is located and whether that data is at rest or in motion.

iii. Generate a hash for each shard: - The blockchain storage system generates a unique hash -- an encrypted output string of a fixed length -- based on the shard's data or encryption keys. The hash is added to both the ledger and shard metadata to link transactions to the stored shards. The exact approach to generating hashes varies from one system to the next.

iv. Replicate each shard: - The storage system replicates each shard so there are enough redundant copies to ensure availability and performance and protect against degradation and data loss. The content owner chooses how many copies to make of each shard and where those shards are located. As part of this process, the content owner should establish a threshold for the minimum number of copies to maintain to ensure against data loss.

V. Distribute the replicated shards: - A P2P network distributes the replicated shards to geographically dispersed storage nodes, either regionally or globally. Multiple organizations or individuals -- sometimes referred to as *farmers* -- own the storage nodes, leasing extra storage space in exchange for some type of compensation, usually cryptocurrency. No one entity owns all the storage resources or controls the storage infrastructure. Only content owners have full access to all their data, no matter where those nodes are located.

vi. Record transactions to the ledger: - The storage system records all transactions in the blockchain ledger and syncs that information across all nodes. The ledger stores details relevant to the transaction, such as the shard location, shard hash and leasing costs. Because the ledger is based on blockchain technology, it's transparent, verifiable, traceable and tamper-proof.

3. How Can Blockchain Be Used in the Real World?

Blocks on the blockchain store data about monetary transactions — we've got that out of the way. But it turns out that blockchain is actually a pretty reliable way of storing data about other types of transactions, as well. In fact, blockchain technology can be used to store data about property exchanges, stops in a supply chain, and even votes for a candidate.

Professional services network Deloitte recently surveyed 1,000 companies across seven countries about integrating blockchain into their business operations. A survey already found that 34% had a blockchain system in production today, while another 41% expected to deploy a blockchain application within the next 12 months. In addition, nearly 40% of the surveyed companies reported they would invest $5 million or more in blockchain in the coming year. Here are some of the most popular applications of blockchain being explored today.

i. Banks:- Perhaps no industry stands to benefit from integrating blockchain into its business operations more than banking. Financial institutions only operate during business hours, five days a week. That means if you try to deposit a check on Friday at 6 p.m., you likely will have to wait until Monday morning to see that money hit your account. Even if you do make your deposit during business hours, the transaction can still take 1-3 days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps. By integrating blockchain into banks, consumers can see their transactions processed in as little as 10 minutes, basically the time it takes to add a block to the blockchain, regardless of the time or day of the week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. In the stock trading business, for example, the settlement and clearing process can take up to three days (or longer, if banks are trading internationally), meaning that the money and shares are frozen for that time.

Given the size of the sums involved, even the few days that the money is in transit can carry significant costs and risks for banks. Santander, a European bank, put the potential savings at $20 billion a year. Capgemini, a French consultancy, estimates that consumers could save up to $16 billion in banking and insurance fees each year through blockchain-based applications.

ii. Cryptocurrency: - Blockchain forms the bedrock for cryptocurrencies like Bitcoin. As explored earlier, currencies like the U.S. dollar are regulated and verified by a central authority, usually a bank or government. Under the central authority system, a user's data and currency are technically at the whim of their bank or government. If a user's bank collapses or they live in a country with an unstable government, the value of their currency may be at risk. These are the worries out of which Bitcoin was borne. By spreading its operations across a network of computers, blockchain allows Bitcoin and other cryptocurrencies to operate without the need for a central authority. This not only reduces risk but also eliminates many of the processing and transaction fees. It also gives those in countries with unstable currencies a more stable currency with more applications and a wider network of individuals and institutions they can do business with, both domestically and internationally (at least, this is the goal.)

iii. Healthcare: - Health care providers can leverage blockchain to securely store their patients' medical records. When a medical record is generated and signed, it can be written into the blockchain, which provides patients with the proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the blockchain with a private key, so that they are only accessible by certain individuals, thereby ensuring privacy

iv. Property Records: - If you have ever spent time in your local Recorder's Office, you will know that the process of recording property rights is both burdensome and inefficient. Today, a physical deed must be delivered to a government employee at the local recording office, where is it manually entered into the county's central database and public index. In the case of a property dispute, claims to the property must be reconciled with the public index. This process is not just costly and time-consuming — it is also riddled with human error, where each inaccuracy makes tracking property ownership less efficient. Blockchain has the potential to eliminate the need for scanning documents and tracking down physical files in a local recording offices. If property ownership is stored and verified on the blockchain, owners can trust that their deed is accurate and permanent.

v. Smart Contracts: - A smart contract is a computer code that can be built into blockchain to facilitate, verify, or negotiate a contract agreement. Smart contracts operate under a set of conditions that users agree to. When those conditions are met, the terms of the agreement are automatically carried out. Say, for example, I'm renting you my apartment using a smart contract. I agree to give you the door code to the apartment as soon as you pay me your security deposit. Both of us would send our portion of the deal to the smart contract, which would hold onto and automatically exchange my door code for your security deposit on the date of the rental. If I don't supply the door code by the rental date, the smart contract refunds your security deposit. This eliminates the fees that typically accompany using a notary or third-party mediator.

vi. Supply Chains: - Suppliers can use blockchain to record the origins of materials that they have purchased. This would allow companies to verify the authenticity of their products, along with health and ethics labels like "Organic," "Local," and "Fair Trade."

vii. Voting: - Voting with blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the November 2018 midterm elections in West Virginia. Each vote would be stored as a block on the blockchain, making them nearly impossible to tamper with. The blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election, and provide officials with instant results.

3.1 Advantages of Blockchain

For all its complexity, blockchain's potential as a decentralized form of record-keeping is almost without limit. From greater user privacy and heightened security, to lower processing fees and fewer errors, blockchain technology may very well see applications beyond those outlined above. Here are the selling points of blockchain for businesses on the market today.

i. Accuracy: - Transactions on the blockchain network are approved by a network of thousands or millions of computers. This removes almost all human involvement in the verification process, resulting in less human error and a more accurate record of information. Even if a computer on the network were to make a computational mistake, the error would only be made to one copy of the blockchain. In order for that error to spread to the rest of the blockchain, it would need to be made by at least 51% of the network's computers — a near impossibility.

ii. Cost: - Typically, consumers pay a bank to verify a transaction, a notary to sign a document, or a minister to perform a marriage. Blockchain eliminates the need for third-party verification and, with it, their associated costs. Business owners incur a small fee whenever they accept payments using credit cards, for example, because banks have to process those transactions. Bitcoin, on the other hand, does not have a central authority and has virtually no transaction fees.

iii. Decentralization: - Blockchain does not store any of its information in a central location. Instead, the blockchain is copied and spread across a network of computers. Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change. By spreading that information across a network, rather than storing it in one central database, blockchain becomes more difficult to tamper with. If a copy of the blockchain fell into the hands of a hacker, only a single copy of information, rather than the entire network, would be compromised.

iv. Efficiency: - Transactions placed through a central authority can take up to a few days to settle. If you attempt to deposit a check on Friday evening, for example, you may not actually see funds in your account until Monday morning. Whereas financial institutions operate during business hours, five days a week, blockchain is working 24 hours a day, seven days a week. Transactions can be completed in about ten minutes and can be considered secure after just a few hours. This is particularly useful for cross-border trades, which usually take much longer because of time-zone issues and the fact that all parties must confirm payment processing.

v. Privacy: - Many blockchain networks operate as public databases, meaning that anyone with an internet connection can view a list of the network's transaction history. Although users can access details about transactions, they cannot access identifying information about the users making those transactions. It is a common misperception that blockchain networks like bitcoin are anonymous, when in fact they are only confidential. That is, when a user makes public transactions, their unique code called a public key, is recorded on the blockchain, rather than their personal information. Although a person's identity is still linked to their blockchain address, this prevents hackers from obtaining a user's personal information, as can occur when a bank is hacked.

Vi. Security: - Once a transaction is recorded, its authenticity must be verified by the blockchain network. Thousands or even millions of computers on the blockchain rush to confirm that the details of the purchase are correct. After a computer has validated the transaction, it is added to the blockchain in the form of a block. Each block on the blockchain contains its own unique hash, along with the unique hash of the block before it. When the information on a block is edited in any way, that block's hash code changes — however, the hash code on the block after it would not. This discrepancy makes it extremely difficult for information on the blockchain to be changed without notice.

vii. Transparency: - Even though personal information on blockchain is kept private, the technology itself is almost always open source. That means that users on the blockchain network can modify the code as they see fit, so long as they have a majority of the network's computational power backing them. Keeping data on the blockchain open source also makes tampering with data that much more difficult. With millions of computers on the blockchain network at any given time, for example, it is unlikely that anyone could make a change without being noticed.

4. CONCLUSIONS

This paper identifies why the blockchain was high at each level during their transactions and also to analysis how to reduce the storage of data. It is useful to understand blockchains in the next context of more valuable crypto currencies, but should not assume that all blockchain ecosystems need bitcoin mechanisms such as proof of work, longest chain rule, etc. Bitcoin is the first attempt at maintaining a decentralized, public ledger with no formal control or governance. There are significant challenges involved.

On the other hand, private distributed ledgers and blockchains can be deployed to solve other set of problems. Blockchain technology could be quite complementary in a possibility space for the future world that includes both centralized and decentralized models. Like any new technology, the blockchain is an idea that initially disrupts, and over time it could promote the development of a larger ecosystem that includes both the old way and the new innovation. This work has achieved promising results, and, in conclusion, is predicted to open a new path for future research related to transferring the protected data in the proceeding for security growth and reduce the data storage .

REFERENCES

[1] Bobby K Simon and Anjana P Nair, "Transferring the Highly Confidential Data in the Fiscal Device Based On BlockChain Security Method," Science, vol. 06, March. 2019, pp. 0056-0072.

[2] Michelle Drolet is founder of Towerwal, a data security services provider in Framingham, MA, with clients such as Smith & Wesson, Middlesex Savings Bank, WGBH, Covenant Healthcare and many mid-size organizations. She can be reached at michelled@towerwall.com.

[3] M. Crosby, Nachiappan, P. Pattanayak, S. Verma,V. Kalyanaraman, "BlockChain technology: Beyond bitcoin", Applied Innovation Review, Berkeley, Issue No.2, June 2016..

[4] https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe.

[5] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System Oct 2008.

[6] Zheng Z, Xie S, Dai H, et al. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends[C]. IEEE International Congress on Big Data. IEEE, 2017.

[7] J. Walker, "The Self-Driving Car Timeline – Predictions from the Top 11 Global Automakers," *TechEmergence*, blog,24August2017;www.techemergence.com/selfdriving-car-timeline-themselves-top-11-automakers.

BIOGRAPHIES

BOBBY K SIMON, received the Bachelor's Degree in Computer Science and Engineering from Karpagam University, TamilNadu, India in 2017. He is currently pursing Master's Degree in Computer Science and Engineering in Sree Buddha College of Engineering, Kerala, India. His research area of interest includes the field of internet security, data mining and technologies in Department of Computer Science and Engineering.

ANJANA P NAIR, received the bachelor's degree in LBS Institute of Technology for Women, Kerala, India. And master's degree in Computer Science and Engineering from Sree Buddha College of Engineering, Kerala, India in 2013. She is a lecturer in the Department of Computer Science and Engineering, Sree Buddha College of Engineering. Her main area of interest is Core Computers and has published more than 10 referred papers.