IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

Blockchain-Based PKI: Making Digital Certificate Management More Secure and Efficient

Sukhvinder Singh Bamber[1], Rajeev Kumar Dang[2], Naveen Dogra[3], Mohit Angurala[4]
Assistant Professor, University Institute of Engineering and Technology,
Panjab University SSG Regional Centre, Hoshiarpur, Punjab, India[1,2,3]
Assistant Professor, Department of Computer Science,
Guru Nanak Dev University College, Pathankot, Guru Nanak Dev University, Amritsar, Punjab, India[4]
ss.bamber@pu.ac.in, dang.rajeev@pu.ac.in, naveendogra@pu.ac.in, and mohit.pathankot@gndu.ac.in

Abstract: *Digital certificates are necessary for encrypting and verifying network communications. As a key part of Public Key Infrastructure (PKI), they check the identities of users, devices, and systems, which is important for network security. This paper looks at digital certificates, what they do, and how important they are for keeping data safe and private. It also talks about how Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols have changed over time and how digital certificates keep online interactions safe. Certificates are very important for managing identities in India, especially in e-government, where they make it possible to safely log in to public services*

Keywords: Digital Certificate; Network Security; SSL-TLS; E-Government; Block-chain based PKI

I. INTRODUCTION

As the internet has grown, it has become more important to protect online communication on both public and private networks. As digital platforms become more important in world economies and governments, it is important to protect data transmission. Digital certificates are a key part of Public Key Infrastructure (PKI) and meet this need. They check the identities of people involved in digital exchanges and stop data from being intercepted and changed. This paper looks at the role, making, and importance of digital certificates in the PKI system for keeping networks safe. It will also talk about the switch from SSL to TLS and how they work together to make web communication secure. The study will also look at how India uses digital certificates in its identity management and e-government systems to make sure that public services are safe and verified.

Digital certificates are electronic documents that prove the identity of a user, server, or device in online transactions. They act like an online passport, making sure that everyone is who they say they are. These certificates are issued by a Certificate Authority (CA), which is a trusted third party. The CA uses its private key to sign the certificate, which proves the holder's identity. A digital certificate usually has important information like the holder's public key, the name of the CA, the date the certificate will expire, and other related information. You can use the public key to encrypt and decrypt data. For instance, your browser checks the digital certificate of a secure website to make sure it is who it says it is. A valid certificate starts an encrypted session, which keeps people from listening in on the data you send to and receive from the site. Digital certificates are a key part of Public Key Infrastructure (PKI). PKI gives you the tools you need to handle digital keys and certificates. PKI helps keep data private, safe, and real by using a mix of asymmetric encryption, certificate management, and other security measures.

Public Key Infrastructure (PKI) uses two keys: a public key that is part of a digital certificate and can be seen by everyone, and a private key that only the certificate holder knows. Only the matching private key can decrypt data that has been encrypted with the public key, and vice versa. This system lets you send data safely, so no one else can get to it. PKI is also what makes digital signatures work, which make sure that data is correct and that the sender is who they say they are. The person who gets a document with a digital signature can check to see if the signature is real. If the signature check doesn't work, it could mean that the data has been changed or that the sender is pretending to be someone else. Digital certificates are a big part of secure web encryption. The first step in the development of these

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, August 2025 Impact Factor: 7.67

protocols was Secure Sockets Layer (SSL), which encrypted data sent between web servers and clients. SSL was good enough at first, but it had flaws that led to the creation of a more secure protocol called Transport Layer Security (TLS). SSL was a good idea, but TLS (Transport Layer Security) is a better and safer version. TLS not only keeps data safe, but it also checks the data as it is sent and makes sure that the people involved are who they say they are. It is an important part of safe web communication that people use to shop, bank, check email, and use cloud services. The s in https:// stands for secure, which means that TLS is being used. The server sends the client (usually a web browser) its digital certificate to show that it is who it says it is. When the browser checks the certificate, it makes a secure link that keeps hackers out and protects communication between servers and clients. Digital certificates are being used more and more in identity management systems to check who you are and make digital services better for users. Digital certificates are used by national ID programs to check who people are when they use government services, pay bills, or access e-governance portals.

Aadhaar is a large biometric ID system that works all over the world and lets national infrastructure use digital certificates. It gives each person a unique 12-digit ID that is linked to their demographics and biometrics. Digital certificates keep data safe by confirming the identities of both users and service providers. Digital certificates check users' public keys to make sure they are real, which limits service access to only verified users. They also check the identities of service providers to stop phishing and fraud. Digital certificates are important for Aadhaar-based services because they keep data safe while it's being sent, which protects users' privacy and stops people from getting into their personal information without permission. These certificates also make sure that users can't deny being involved in a transaction because their digital signatures can be verified.

Digital certificates and Public Key Infrastructure (PKI) make security better by making sure that data is correct, users are who they say they are, and they can't deny it. Digital services are becoming more common in both business and government, which will likely lead to a rise in the need for digital certificates. Digital identities, e-governance, and easier online transactions are becoming more popular around the world. This shows how important it is to have strong security systems, which makes digital certificates even more important.

Digital certificates need to change as technology improves, like quantum computing, which could make current encryption methods useless. To make sure that digital certificates stay a safe way to communicate in the future, researchers are working on quantum-resistant algorithms and new PKI standards.

II. REVIEW OF LITERATURE

Fan et al. (2019) examined the possibilities of blockchain for the issuance and validation of digital credentials. Their research demonstrated that blockchain technology enhances the security, transparency, and permanence of certificate management. Blockchain allows for a decentralized approach by getting rid of the central control and inefficiencies that are common in standard PKI systems. This builds trust by making sure that the data is correct and giving an unchangeable record of transactions, which makes people more confident in the certification process. In 2020, Shen J. et al. introduced a blockchain-centered Public Key Infrastructure (PKI) for IoT devices. Their system used a decentralized management style that worked well for IoT settings and focused on improving privacy and security. The architecture was made to work with big IoT networks, allowing for decentralized and secure certificate management while reducing the number of single points of failure. Abouelseoud et al. (2020) suggested using blockchain technology to make managing certificates in cloud computing environments safer. Their method worked especially well for dealing with security problems that came up when issuing, storing, and revoking certificates. The unchangeable and clear nature of blockchain was used to protect cloud certificates from being changed without permission and to speed up the process of revoking them. Xia C. et al. (2021) discovered that blockchain technology can facilitate a Public Key Infrastructure (PKI) system for the management of digital certificates efficiently while accommodating scalability. Their research emphasized that scalability is essential as network infrastructures and IoT configurations expand. They proposed a system that could quickly and safely handle many certificates, which shows that blockchain could be useful for reliable, distributed management. Attiya G. et al. (2021) examined the utilization of blockchain technology for certificate management to bolster the security of IoT communications. Their research demonstrated that the integration of decentralized methodologies could alleviate scalability and security issues within IoT communication protocols. The

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

system they proposed used blockchain to protect against problems with central control and possible attacks. This made the network environment for IoT devices more stable and secure. Zhou H. et al. (2022) put forward a blockchain-based system for quickly revoking certificates that has a ledger that can't be changed and is open to everyone. Their design fixes common problems with standard PKI systems, like revocation processes that don't work or are too hard to use. The system uses blockchain's distributed ledger to make sure that certificate statuses are updated in real time and can be accessed by all necessary parties. This makes revocation quick. Li C. et al. (2020) put forward a decentralized public key infrastructure (PKI) for IoT networks that is based on blockchain technology. This system is meant to solve problems with data integrity, privacy, and scalability that are unique to IoT environments. The system protects certificate data from being changed by taking advantage of blockchain's decentralized nature and creating an audit trail that can be checked to build trust. Li et al. (2021) proposed applying blockchain tech to manage digital certificates within 5G networks. Their system made it easier to issue, check, and revoke certificates, which made 5G communications safer. The fact that blockchain is a distributed ledger makes it harder for certificate data to be corrupted or misused, which makes these advanced networks more reliable. Portugal P. P. et al. proposed a blockchain-based PKI framework for IoT devices in 2020. The goal of the study was to make digital certificates more scalable, clear, and trustworthy. The framework tried to use blockchain to handle a lot of certificate operations safely and openly, which is very important for IoT setups that are spread out. L. M. Galindo and others made a blockchain-based public key infrastructure (PKI) in 2020 to make the process of revoking certificates faster and better. The system keeps a verifiable history of certificate statuses by using blockchain's immutable ledger. This makes revocation management more open and safe. This method makes certification more trustworthy and protects the system by stopping changes that aren't allowed. Yang H.E. and Lin T. made a simple blockchain system for revoking certificates in car networks in 2019. Their main goal was to make revocation happen quickly and safely, which is important for sharing data between connected cars in real time. Blockchain technology made it possible for cars to communicate with each other quickly and reliably, which helped with both safety and proper operation. Yadav P.S. (2023) proposes an automated system for managing the lifecycle of certificates in modern IT infrastructures. Certificates are very important for secure communication and authentication, so managing their lifecycle is very hard. The proposed system uses automation to make it easier to get, deploy, monitor, and renew certificates in order to make these problems easier to deal with. Initial findings indicate that the method enhances certificate management within organizations via source analysis, system design, and empirical testing, simultaneously mitigating the risk of human error, thereby augmenting overall security. Atutxa A. et al. (2023) examined a system for validating server certificates within a network. This system uses data plane programming (DPP) to move the validation work from Industrial Internet of Things (IIoT) devices that don't have enough resources to a network element that can handle it. This method makes things safer by requiring server certificate checks and faster by moving resource-heavy tasks to other servers. The findings indicate a 50% to 60% decrease in the time it takes to set up a Datagram Transport Layer Security connection and a 40% decrease in CPU usage on IIoT devices, which saves power. Zhang J. et al. (2014) created a model for setting prices and taking away certificates authorities (CAs) that takes into account how users make decisions. This model answers two main questions: What should the cost of digital certificates be for CAs? Researchers suggested that the cost of a digital certificate should be based on the possible financial losses to the user's IT system due to security issues. The study also says that the number of times certificates are revoked goes down as they get older. This is backed up by real-world data from VeriSign. The authors suggest that CAs use a dynamic certificate revocation list (CRL) policy, which means that the best time to release a certificate gets longer as it gets older. Costa D. et al. (2022) have made a blockchain system for the Internet of Things. This system is safe, can be added to, and can be made bigger. It also lets factories today quickly approve production data. The structure has everything you need to keep an eye on network tasks. The system could connect to current factory tools thanks to special APIs. This made it easy to add to the platform, which cut down on the amount of setup needed for hardware or software. Authors proposed a working model to test the solution and make sure that the design could be used to quickly and safely certify manufacturing data. The development of blockchain-based public key infrastructure was made possible by a survey of the literature.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

III. PROBLEMS AND DRAWBACKS OF DIGITAL CERTIFICATES

Digital certificates are very important for network security and authentication, but they do come with some problems. To keep certificates safe and reliable, we need to get past a few problems.

A. Compromise of the Certificate Authority

How much people trust Certificate Authorities affects how safe the digital certificate system is. If a CA gets hacked, it can give out fake certificates that let attackers act like real people. Attacks on well-known CAs like DigiNotar and Comodo are some of the most famous ones. Because of these attacks, fake certificates were made for well-known websites. Some ways to lower these risks include Multi-Factor Authentication (MFA) for CAs and Decentralized Solutions:

- Multi-Factor Authentication (MFA) for CAs: By using MFA to make CAs' security stronger, you can make it less likely that they will be hacked.
- Decentralized Solutions: New technologies, like blockchain, could help spread the trust mechanisms across many nodes, so that people don't have to rely on just one point of failure.

B. Taking Away a Certificate

Another big problem is how to manage certificate revocation in a way that works well. If a certificate is stolen, it needs to be revoked right away to stop it from being used for bad things. Checking Certificate Revocation Lists (CRLs) or the Online Certificate Status Protocol (OCSP), on the other hand, can slow down communication, which can make the system work less well and hurt the user experience. How well do services that cancel things work? One possible solution to these problems is to speed up and make OCSP Stapling and other revocation mechanisms more reliable. OCSP Stapling lets servers store and send the status of certificates.

C. Surveys and statistical studies on the use of digital certificates

Adding a part that talks about survey data and statistical analysis will back up the claims that digital certificates are very important and widely used. For instance, cybersecurity groups might do surveys and find that 80% of banks use digital certificates to keep their transactions safe. Adding information about how much people trust things, like how much the public trusts Certificate Authorities (CAs) or how reliable they think digital certificates are, will give more depth and show how people around the world see digital certificates.

D. Problems with Recognizing Certificates Across Borders

One of the biggest problems with digital certificates is that they aren't always accepted the same way in different places. This issue happens because the PKI standards in different countries may not be the same. This means that a digital certificate that is trusted in one country may not be trusted in another. This makes it hard to talk to people across borders digitally. To fix these issues, we need to make the rules more consistent and set up global trust frameworks. Working together to standardize PKI practices across countries can help certificates be recognized across borders. This will make it safer and more unified for people to interact online all over the world.

IV. NEW TRENDS AND FUTURE OF DIGITAL CERTIFICATES

The role of digital certificates changes as the world of cybersecurity changes. New technologies like quantum computing and blockchain, as well as the growing need for decentralized security systems, will have an impact on the future of digital certificates and Public Key Infrastructure (PKI).

A. Quantum Computing and PKI Changes

So, the problem is quantum computing: quantum computers will break cryptographic algorithms that are used a lot. The problem in the near future is that once quantum computers get strong enough, they can quickly break the RSA and ECC algorithms. This puts the whole PKI framework's security at risk.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

Algorithm of Shor

This is a quantum algorithm that can break down big numbers very quickly. It goes against RSA encryption in every way. So, PKI would be greatly affected because most of the digital certificates that were issued, verified, and revoked would be at risk.

Post-Quantum Cryptography (PQC)

The study of PQC is based on figuring out which algorithms can stand up to quantum attacks. Some examples are lattice-based cryptography, multivariate polynomial cryptography, and code-based cryptography. This means that post-quantum cryptography will have to be used to change how certificates are issued, verified, and revoked in PKI setups.

Quantum-Safe Transition Plans

Organizations can use the hybrid cryptography approach, which combines classical algorithms with quantum-resistant ones. This method is backward compatible because it has two parts, and it has quantum-safe features.

B. Blockchain and Decentralized Public Key Infrastructure (DPKI)

Blockchain-based innovation for PKI gives decentralized PKI the power to get around the problems that come with centralized control and CA misbehaviour. Immutable Certificate Management: An append-only ledger can be used to share certificates in a decentralized way using blockchain. Each time a certificate is issued or revoked, it is recorded as transactional data on that network. This ensures transparency and prevents any changes from happening from unauthorized sources.

Model of High Security

The fact that blockchain-based PKI doesn't depend on a single point of authority for execution is one of the most important differences between it and traditional PKI. Trust is spread out among the nodes in a network, which makes it less likely that attacks or failures will happen. You can use smart contracts to automate tasks related to certificates, like renewing or cancelling them.

Reducing the risks of CA compromise

PKI frameworks built on blockchain make sure that the system stays safe even if part of the network is hacked because consensus protocols require most nodes to agree.

C. Artificial Intelligence and Machine Learning in PKI

Here are some ways that AI and machine learning are being used to better handle digital certificates:

Finding Unusual Events

ML-based algorithms can keep an eye on how certificates are used and find any strange behaviour that could lead to losing control of that certificate or fraud happening. This could stop them from being misused or lead to users getting certificates that aren't real.

Renewals that are based on predictions

AI and ML-enabled platforms can automatically start the renewal process when a certificate is about to expire, which cuts down on the time that services are unavailable.

Finding Phishing and Fraud

ML models can find and mark sites that use fake or rogue certificates as phishing. This protects users better because it stops bad sites before they can do any damage.

D. New Ways to Revoke Certificates

There are always new solutions that make the two traditional ways of revocation—CRLs and OCSP—better:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, August 2025 Impact Factor: 7.67

Revocation Based on Blockchain

You can safely store updates about the status of certificates in real time on a distributed ledger. When this method is used, it gets rid of the latency and scalability problems that come with traditional CRL and OCSP. The network shows the removed certificates right away.

Merkle Trees for Quick Revocation

Using data structures like Merkle trees makes it easier to check statuses. Verifiers have proof of revocation with little data retrieval, so the checks are faster and more reliable.

E. Web 3.0 and Self-Sovereign Identity (SSI)

Decentralization, which is at the heart of Web 3.0, goes very well with PKI innovation that lets users control their data. The SSI framework uses blockchain to create and check credentials, so it doesn't need any central authorities. With an SSI model, users would be able to control their digital identity and prove it with credentials based on blockchain technology. This would make people less reliant on government or corporate identity providers, which would give them more privacy and security. Countries like India can use SSI to make digital identity systems more open and honest, while still giving the right people control over their credentials and keeping high levels of verification.

F. Combining IoT and Edge Computing

IoT devices are hard to use in PKI environments because they are often deployed in places with limited resources. PKI can only protect future IoT communications if it can handle ECC, lightweight post-quantum cryptography, and more efficient algorithms that provide the same level of security with less computational overhead, so devices don't have to deal with the resulting slowness. Edge-Based PKI Management lets local edge nodes take over certificate management tasks from central servers. This also speeds up the time it takes to issue and revoke certificates. The latter also adds security by spreading out tasks.

G. Making Certificate Lifecycle Management Automatic

When there are a lot of systems, it is not possible to manage certificates by hand. A lot of automation tools handle the whole lifecycle, from issuing a certificate to renewing it and revoking it. The most advanced systems can automatically issue certificates, keep track of when they expire, and renew them without any help from people. This stops service interruptions that happen when certificates expire. Advanced Security Policies: Automation software can enforce strict security policies by issuing certificates based on the needs of the organization, following best practices, and so on.

What will happen next?

Distributed ledger technologies that go beyond blockchain. Blockchain is the most popular DLT, but Hashgraph and DAGs are also getting a lot of attention and are good options for managing PKI. Hashgraph is better for real-time PKI operations that need low latency because it has faster consensus times than a blockchain. Because of how DAG-based systems work, IOTA's Tangle will be able to handle many more transactions without compromising security. This is of course better for managing a lot of certificates in environments where devices are very interconnected. PKI changes to keep up with the needs of a world that is becoming more connected and security-conscious. In the future, PKI will be quantum-resistant, blockchain-based for transparency, and machine learning-based for automation.

V. DIGITAL VERIFICATION AND CERTIFICATION

Diffie and Hellman's idea of public-key cryptography in the 1970s led to the creation of Public Key Infrastructure (PKI). Before their invention, it was hard to securely share encryption keys, which made digital communication less secure. Their work led to the development of modern PKI systems that handle digital certificates and the public-private key pairs that go with them. In the 1990s, Secure Sockets Layer (SSL) was created to protect online transactions. It later became Transport Layer Security (TLS) to fix security problems. This change shows that PKI can change with the times and meet new security needs.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

A. Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) gives you a way to make, manage, share, and cancel digital certificates. PKI makes sure that communication on open networks like the internet is safe and verified by protecting privacy, accuracy, and identity. Identity confirmation makes sure that the people who are talking to each other are who they say they are. It includes these steps:

- *Privacy*: Encrypts data so that only people who are allowed to see it can.
- *Integrity*: Makes sure that the data stays the same while it's being sent.
- *Non-Repudiation*: Makes it impossible for one party to say they didn't take part in the communication.

B. Using Digital Certificates for Authentication

Digital certificates are very important for making sure that the people who are talking to each other are who they say they are. This is how authentication works:

- *Checking someone's identity*: The CA checks the certificate's public key to make sure it is valid, which proves who the entity is.
- *Building Trust*: The certificates build trust between the people who are talking because they are made or given out by a trusted authority.
- *Exchange of Secure Keys*: The certificate's public key lets you share keys safely during SSL/TLS handshakes and other sessions that are encrypted.
- *More complex PKI models*: Fig. 2 (flowchart) shows how blockchain's decentralized and tamper-proof ledger makes it easier to issue, validate, and revoke certificates.

VI. SECURED SOCKET LAYER (SSL) AND TRANSPORT LAYER SECURITY (TLS)

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are two encryption protocols that keep online communication safe. Netscape started working on SSL in the mid-1990s to make sure that communications between clients and servers were safe. After many revisions, changes, and patches to fix security holes in SSL, the newer, better, and more reliable version, TLS, came out. TLS is now the standard way to protect web communications. SSL, on the other hand, is no longer used because it is vulnerable to attacks like POODLE and BEAST. Both protocols make communication safer by giving:

- *Confidentiality* means making sure that data that is sent is encrypted and can only be read by people who have permission to do so.
- *Integrity* means making sure that the data hasn't been changed or messed with while it was being sent.
- *Authentication* is the process of checking that the people who are talking to each other are who they say they are.

The Internet Engineering Task Force (IETF) made the TLS protocol in 1999 to deal with growing security issues with SSL. The goal of TLS 1.0 was to be a safer version of SSL 3.0. Later versions, like TLS 1.1, 1.2, and 1.3, added more security features, like stronger encryption, better key exchange methods, and the removal of old algorithms. TLS 1.0 (1999) fixed cryptographic flaws and worked with older systems, making it better than SSL 3.0. TLS 1.1 (2006) fixed issues with the initialization vectors for block ciphers, making them less likely to be attacked by things like BEAST. TLS 1.2 came out in 2008 and added support for more secure cryptographic hash functions like SHA-256. It also made authenticated encryption better. TLS 1.3 (2018) made the handshake process easier, faster, and safer. It also stopped supporting older, less secure algorithms, which helped with speed and security.

SSL/TLS needs digital certificates to work. These protocols check the identities of servers and sometimes clients, and they help make key exchanges safe. Trusted third-party Certificate Authorities (CAs) give out certificates. These certificates have a public key that clients use to check the server's authenticity during the SSL/TLS handshake. The SSL/TLS handshake is a set of steps that make sure the client and server can talk to each other safely. In this step, both sides agree on how to encrypt data, verify the server (and optionally the client), and make a session key for secure communication.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, August 2025 Impact Factor: 7.67

Algorithm 1: The SSL/TLS Handshake

Hello, Client

The client sends a message to the server here that tells it what the SSL/TLS versions can do, what ciphers they support, and a random number for seeding (to make keys for sessions).

Hello, Server

The server sends back a message that lets you choose a protocol version and a cipher suite, which is an encryption algorithm that the server is ready to use. The server also sends a random number.

Certificate

The server has its own certificate that has a public key on it. The client will use this certificate to make sure the server is who it says it is.

Key Exchange

The client makes what is called a "pre-master secret" and encrypts it with the server's public key, which is printed on the certificate. The server will use its private key to unlock this pre-master secret.

Making a Session Key

Both the client and the server make a session key on their own using the pre-master and the random numbers that were sent earlier. The session key that was made is then used to encrypt the data that is being sent during the conversation.

Client Done

The client sends a message that has been encrypted with the session key, letting the other side know that the handshake is complete on its side.

Server Done

The server sends an encrypted message with the same session key to let the client know that the handshake is complete on its end. After the handshake is over, both the client and the server use the session key to encrypt the rest of the communication.

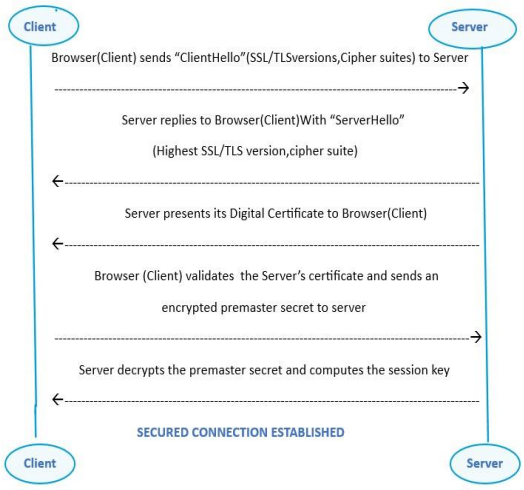

Fig. 1: The SSL/TLS Handshake Process

Pseudocode for the SSL/TLS Handshake Process

SSLTLS Handshake *(client, server)*
client.send *(Client Hello (list of Supported Protocols, list of Supported Cipher Suites))*
server.send *(Server Hello (chosen Protocol, chosen Cipher Suite))*
server.send *(Certificate (Public Key of Server))*
if ***client.validate Certificate*** *(Certificate) is true then*

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, August 2025 Impact Factor: 7.67

Make a Premaster Secret and then set it to Premaster Secret.
Encrypted Secret *← encrypt (server Public Key, Premaster Secret)*
client.send *(Secret Encrypted)*
session Key *← get Session Key (Premaster Secret)*
client.send *(encrypt ("Handshake complete", session Key))*
server.send *(encrypt("Handshake complete", session Key))*
return *"Successfully set up a secure connection"*
else
return "Certificate validation failed"
end if
end

SSL/TLS Cipher Suites: These are groups of protocols that tell SSL/TLS how to encrypt, verify, and authenticate data during communications. Encryption tools like:

- *Key exchange algorithm*: This is what you use to send secure keys (like RSA, DH, and ECDH).
- *An encryption algorithm* is a set of rules that tell a computer how to encrypt data. Examples include AES, 3DES, and ChaCha20.
- *Message Authentication Code (MAC) Algorithm* makes sure that data is correct (for example, HMAC with SHA256).
- *Cipher suites* change as TLS gets newer versions. For instance, TLS 1.3 uses cipher suites that are stronger and more efficient than those in TLS 1.2.

The move to TLS was made because SSL had a number of flaws, including POODLE, BEAST, and Heartbleed. These attacks took advantage of flaws in how encryption works or how protocols are made. TLS fixed these problems by:

- Getting rid of weak cipher suites.
- Adding elliptic curve cryptography to make key exchange better.
- Making the handshake process in TLS 1.3 simpler to protect against some attacks, like man-in-the-middle.

Digital certificates support SSL/TLS, which is still one of the most important technologies for keeping internet communications safe. The change from SSL to TLS has made web transactions much safer by making sure that communications are encrypted and that strong authentication methods are used. But you should always be on the lookout, especially with new threats like quantum computing. This could mean that encryption protocols need to be updated in the future.
Fig. 2, Fig. 3, Fig. 4 and Fig. 5 (Flowcharts) describes how PKI structures work and how SSL and TLS protocols keep communications safe. Fig.2 shows the PKI hierarchy, from the root CA to the end-entity certificate, and explains the trust chain in PKI better. Fig. 3 shows each step of the SSL/TLS handshake, from the client's first "hello" to the start of a secure session, also makes it easier to understand the process.

VII. SUGGESTED MODEL

Blockchain-based Public Key Infrastructure (PKI) is a combination of PKI features and blockchain technology that solves problems that have been around since the 1970s in certificate authority systems. In the past, relying on certificate authorities to distribute certificates made systems more vulnerable, with problems like single points of failure and security breaches. Bitcoin, which came out in 2008, was the first to use blockchain technology. Its goal was to create an unchangeable ledger for clear transaction and data management.
The first studies into ways to get certificates started in the 2010s, which led to more people using them. Later, blockchain-based PKI came out as a new way to use contracts to automate the issuance and revocation of authentication certificates. Blockchain-based PKI is now seen as a way to make digital certificate management safer and more decentralized, even though it has some problems, such as not being able to handle large amounts of data and not having

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

clear rules. The Blockchain-Based (PKI) model uses the fact that blockchain is decentralized and can't be changed to solve problems with traditional PKI. This explains how this model works:

In a decentralized setting, it is easier to issue, check, and revoke certificates. Some people suggest using a Blockchain-Based Public Key Infrastructure (PKI) to solve today's problems. This method takes advantage of blockchain's built-in strengths, like decentralization, immutability, and transparency, to make managing certificates easier. Blockchain-based PKI does away with the need for a central authority by using a distributed ledger. This makes handling digital certificates more secure and reliable.

The decentralized method makes the system more secure and able to grow. The system becomes more automated and open by combining smart contracts with tokenization. These improvements make it less likely that people will make mistakes or try to change things, which makes managing certificates more reliable and efficient. Fig. 2, Fig. 3, Fig. 4 and Fig. 5 shows the blockchain-based Public Key Infrastructure (PKI) model. They explain how to issue, validate, and revoke certificates to make things safer and more open.

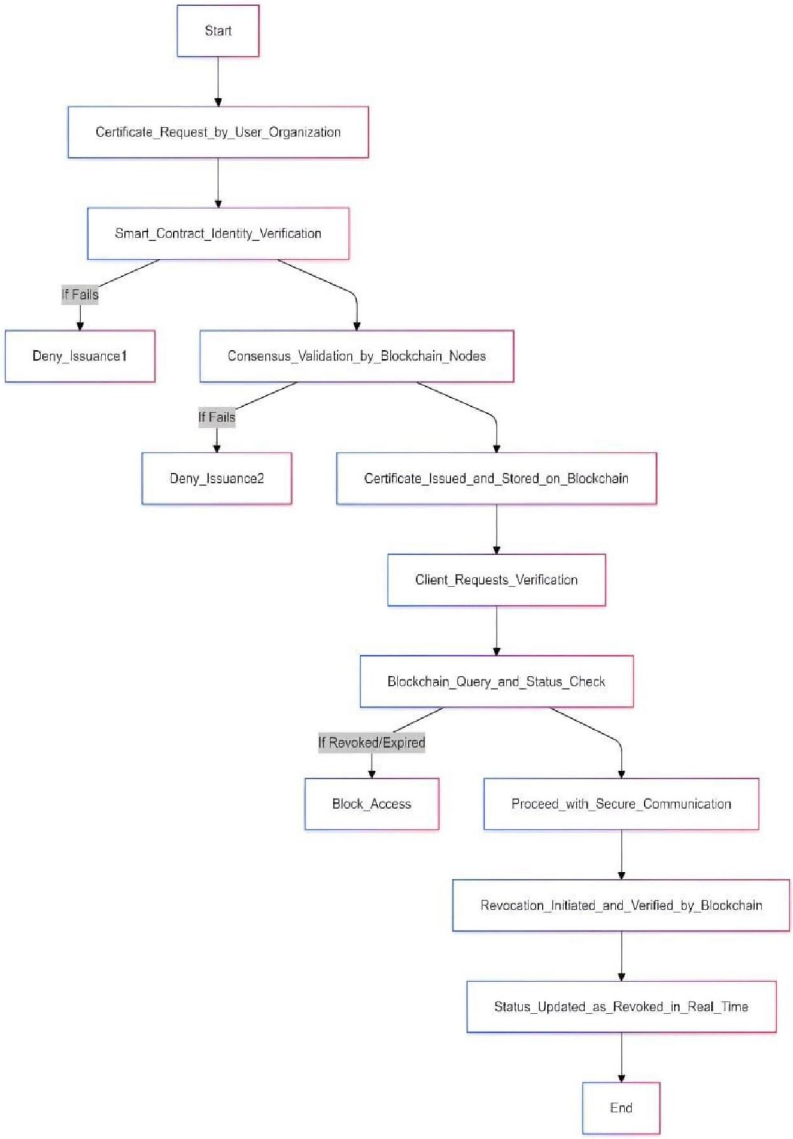

Fig. 2: Steps for issuing, validating and revoking certificates to make things safer and more open.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

A. Getting a Certificate

Smart contracts make it easy and safe to issue certificates in blockchain-based Public Key Infrastructures (PKIs). This is how the process works:

- *Certificate Request*: The blockchain network gets a request from each party, along with their public key and other identifying information.
- *Smart Contract Verification*: Smart contracts can check identities automatically by getting information from other places.
- *Agreement Validation*: The nodes on the network check the transaction and then agree to let it happen.
- *Making a Certificate Record*: After the verification is successful, the certificate is issued and added to the blockchain as a block. The block has important information like the name of the issuer, the certificate holder's information, the public key that goes with it, and the time it was issued.
- *Completion*: The blockchain has stored the certificate, so users can check it whenever they want.

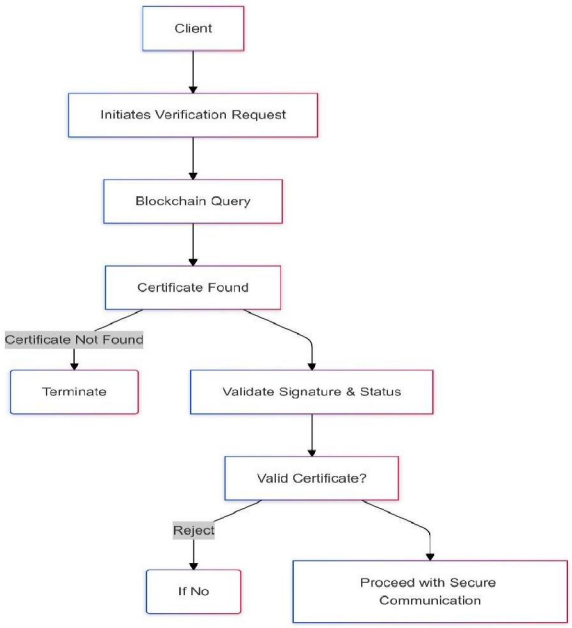

Fig. 3: The steps to getting a Certificate

B. Checking the Certificate Process

Verification makes sure that a server or user certificate is real and hasn't been changed in any way and consists of the following:

- *Verification Request*: The client asks the blockchain for a certain certificate to start a verification request.
- *Blockchain Query*: The system looks in the blockchain and finds the certificate you wanted.
- *Certificate Validation*: The client uses the CA's public key, which is stored in the blockchain, to check the certificate information and the digital signature.
- *Check Certificate Status*: The blockchain record shows you the status (valid, expired, or revoked).
- *Completion*: The certificate is used to send secure messages if it is valid. If not, the connection is lost.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

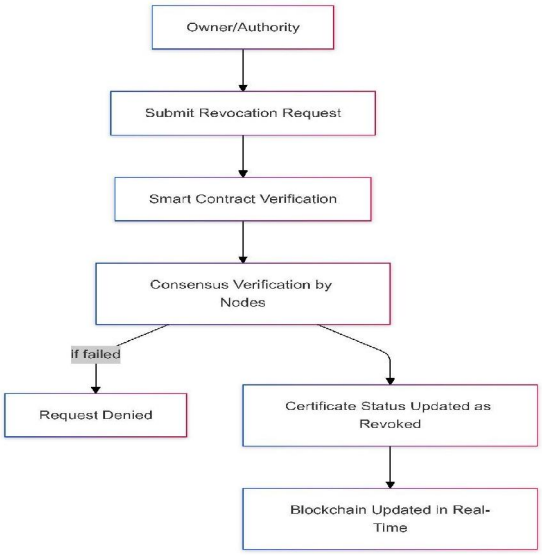

Fig. 4: How to Check a Certificate

C. Process of Revoking a Certificate

Revocation in blockchain-based PKI works well because it keeps the network up to date with compromised or expired certificates in real time.

- *Revocation Request*: The owner or an authority asks for the certificate to be revoked because it has been compromised or has run out of time.
- *Execution of the Smart Contract*: A smart contract takes care of the request to revoke and makes sure it is allowed.
- *Consensus Verification*: The nodes in the blockchain make sure that the revocation is real.
- *Update Blockchain Record*: The blockchain shows that the certificate has been taken away. Completion: Anyone who looks up the certificate can easily see if it has been revoked.

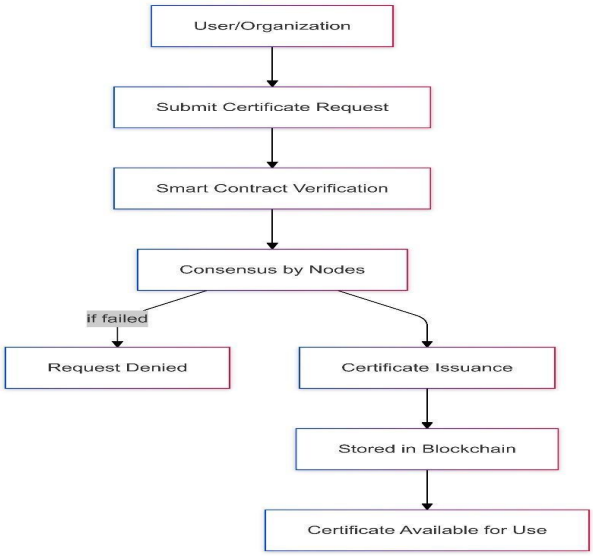

Fig. 5: How to Revoke a Certificate

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

VIII. BENEFITS OF PKI MODEL BASED ON BLOCKCHAIN

- *Tamper-Proof*: Blockchain records that can't be changed or used in the wrong way keep certificates safe.
- *Transparency*: You can easily see all certificate transactions, so it's easy to see any actions that are against the rules.
- *Automated Processes*: Smart contracts automatically issue and cancel contracts, which makes it less likely that people will make mistakes.
- *Real-time updates*: Anyone on the network can see right away when a certificate's status changes.

IX. FUTURE SCOPE FOR IMPROVED BLOCKCHAIN BASED PKI MODEL

- *Multi-Chain Framework for Better Security:* By combining public and private blockchains, a multichain structure can make a blockchain PKI model more secure and flexible. Public blockchains can make it easy to see when certificates are issued and updated. Private blockchains can keep sensitive tasks and logs from being accessed by anyone who shouldn't be able to. This mix of public chain openness and private chain security makes the PKI system safer and more flexible.
- *Managing Certificates in Layers:* A tiered approach to certificate governance can be implemented by classifying them according to their security level and intended use, such as high-assurance and standard certificates. This structure makes it easier to apply the right security protocols to different types of certificates. Sharding helps with scalability because it lets each tier handle requests on its own, which keeps the network stable.
- *Self-Auditing and Following the Rules*: Adding automated compliance checks to smart contracts can make them more reliable and clear. These contracts can check credentials from time to time to make sure they follow rules like GDPR. One can add real-time compliance reporting features so that regulatory bodies can see audit logs directly. This automation lowers the chance of human error and manual verification, which makes people more likely to trust the system.
- *Advanced Ways to Revoke*: Adding options for partial or time-based certificate revocation could make the model better. The partial option lets you turn off some certificate features or apps while keeping the main function available. This is helpful when you need to deal with certain security risks. The time-based option puts a certificate on hold for a set amount of time, after which it automatically turns back on. This is helpful for planned maintenance or temporary security problems.
- *Strategies for putting it into action*: To improve the usefulness of blockchain-based PKI models, several strategies should be thought about: personalization of consensus mechanisms, decentralized storage solutions, incorporation of quantum-safe cryptography, utilization of machine learning for anticipatory security measures, and augmentation of user privacy controls.

As quantum computing gets better, it's more and more important for the model to use quantum-resistant cryptography to stay useful in the long run. Adding support for IoT devices and 5G networks to blockchain-based PKI can also make it more useful by making it possible for new technologies to communicate securely.

Table 1: PKI that is based on blockchain vs. PKI that is based on traditional methods

Process	Traditional PKI Approach	Blockchain-Based PKI Approach
Certificate Issuance	Centralized Certificate Authority (CA) Issues certificates; requires manual validation.	Decentralized validation through blockchain network nodes. Smart contracts automate issuance criteria, ensuring certificates meet set standards without manual.
Certificate Verification	Verifiers (e.g., businesses) must contact CA for certificate validation; delays and reliance on intermediaries.	Verifiers can query the blockchain to instantly check a certificate's validity, status, or expiration. Transparency across nodes enables real-time, reliable

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

		verification without intermediary involvement

This paper proposes a model in which a blockchain-based Public Key Infrastructure (PKI) serves as an alternative to conventional digital certificate systems. Certificate issuance, validation, and revocation in traditional PKIs rely on central authorities, which can lead to problems with security, scalability, and operational speed. A blockchain-based PKI, on the other hand, spreads trust across a network, making it possible to manage certificates without a central authority.

Blockchain technology makes a record that everyone on the network can see and that can't be changed. The system keeps a secure record of when a digital certificate is issued, changed, or revoked across the network. This method keeps things open and lets changes be made in a controlled way. It cuts down on the chances of fraud and data manipulation by checking and recording each action on multiple nodes. It also gets rid of single points of failure. Blockchain uses cryptography to make it harder for people to change or make up records without permission.

A Public Key Infrastructure (PKI) that is based on blockchain technology has advantages for managing digital certificates. First, it makes things faster and more efficient by updating and verifying information in real time. Second, blockchain's decentralization and cryptographic protections make it safer by stopping unauthorized access and changes to data. Third, more openness lets network participants check certificates, which makes the environment more trustless by lowering centralized control. A blockchain-based PKI makes it easier, safer, and more open to handle digital certificates. It spreads trust throughout the network, making it less reliant on central authorities. This makes the system more resilient, scalable, and able to meet future digital security needs

X. CONCLUSION

Digital certificates are very important for making sure that communication is safe in today's digital world. It gives you the tools you need to make sure that authentication, privacy, integrity, and non-repudiation are all in place for a wide range of applications, from Aadhaar, India's national identity management system, to safe web browsing. Digital certificates will need to change as cyber threats become more intelligent. In the future, quantum computing, blockchain, and machine learning will all change how certificates are handled. We need to get ready for quantum-resistant encryption, look into decentralized PKI models, and use automation to keep the trust and security that digital certificates give us. India's quick move to digital, especially in its egovernance and identity infrastructure, shows how important it is to have good certificate management. As projects like DigiLocker, eSign, and Aadhaar grow, cybersecurity needs will change. To keep up with these changes, we will need digital certificate frameworks that are safe, scalable, and flexible. How well centralized control, decentralized trust models, and new cryptographic technologies work together will determine the future of digital certificates.

REFERENCES

[1]. Fan S., Wang Y. and Li M. (2019), ‘‘A Blockchain-Based Digital Certificate Issuing and Verification System’’, *IEEE Access*, Vol. 7, pp. 1234–1245.

[2]. Shen J., Han Y., Liu X. and Ma Y. (2020), ‘‘Blockchain-Based Public Key Infrastructure for Digital Certificates in IoT Devices’’, *IEEE Internet of Things*, Vol. 7, No. 3, pp. 2565–2576.

[3]. Abouelseoud M., Ali A. H. and Rizk K. A. (2020), ‘‘Enhancing Security of Digital Certificates in Cloud Computing Using Blockchain’’, *IEEE Transaction on Cloud Computing*, Vol. 8, No. 2, pp. 560–571.

[4]. Xia C., Wang Z. and Zhu T. (2021), ‘‘Designing a Secure and Scalable Blockchain-Based Public Key Infrastructure’’ *IEEE Transactions on Information Forensics and Security*, Vol. 16, No. 4, pp. 1332–1345.

[5]. Attiya G., Ahmed S. and Joshi P. K. (2021), ‘‘Securing IoT Communications with Digital Certificates Using Blockchain’’, *IEEE Transactions on Emerging Topics in Computing*, Vol. 9, No. 2, pp. 230–242.

[6]. Zhou H. and Yang X. (2020), ‘‘Revoking Digital Certificates Efficiently Using Blockchain Technology’’, *IEEE Network*, Vol. 34, No. 5, pp. 127–134.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

[7]. Li C., Zhao J. and Huang F. (2020), ''Blockchain-Based Decentralized Public Key Infrastructure for IoT Networks'', *IEEE Transactions on Industrial Informatics*, Vol. 16, No. 10, pp. 6602–6612.

[8]. Li L., Wei H. and Chen J. (2021), ''Blockchain-Based Authentication for Digital Certificates in 5G Networks'', *IEEE Communications Magazine*, Vol. 59, No. 3, pp. 44–51.

[9]. Portugal P. P., Silva M. and Costa R. (2020), ''An Efficient Blockchain-Based PKI Management Framework for IoT Devices'', *IEEE Access*, Vol. 8, pp. 13476–13487.

[10]. Galindo L. M., Sosa R. R. and Rivera, M. T. (2020), ''A Blockchain-Based Approach for Revocation Transparency and Digital Certificate Integrity in PKI Systems'', *IEEE Transactions on Engineering Management*, Vol. 67, No. 3, pp. 800–812.

[11]. Yang H. E. and Lin T. (2019), ''Lightweight Blockchain-Based Certificate Revocation Mechanism for Vehicular Networks'', *IEEE Access*, Vol. 7, pp. 84065–84075.

[12]. Yadav P.S. (2023), "Automation of Digital Certificate Lifecycle: Improving Efficiency and Security in IT Systems", *Journal of Mathematical & Computer Applications*, ISSN: 2754 – 6705, Vol. 2, No. 2, pp. 1-4.

[13]. Atutxa A., Astorga J., Barcelo M., Urbieta A. and Jacob E. (2023), "Improving Efficiency and Security of IIOT Communications Using In – Network Validation of Server Certificate", *Computers In Industry, Elsevier*, Vol. 144.

[14]. Zhang J., Hu N. and Raja M.K. (2014), "Digital Certificate Management: Optimal Pricing and CRL Releasing Strategies", Decision Support Systems, Elsevier, Vol. 58, pp. 74 – 78.

[15]. Costa D., Teixeira M., Pinto A.N. and Santos J. (2022), "High – Performance Blockchain System for Fast Certification of Manufacturing Data", *Discover Applied Sciences, Springer*, Vol. 4, No. 25.