The International Journal of Engineering and Science (IJES)
|| Volume || 14 || Issue || 4 || Pages || PP 78-81 || 2025 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Blockchain-Based Authentication for Education: A Secure DLT Framework in India

Dr. Ayaz Ahmed Faridi
Assistant Professor CS & IT ayazahmed.faridi@kalingauniversity.ac.in

Amanuwell Lakra
Student B.Tech C.S.E 8th sem

Samir Kumar Paswan
Student B.Tech C.S.E 8th sem

Ravi Upadhyay
Student B.Tech C.S.E 8th sem

Rachit Sachdeo
Student B.Tech C.S.E 8th sem

ABSTRACT

India face escalating cyber threats amid rapid digitization. Traditional password- based logins are proving inadequate, with frequent data breaches and credential leaks putting student and faculty data at risk. This report explores a blockchain- based authentication framework leveraging Distributed Ledger Technology (DLT) to enhance security over conventional logins. We compare the traditional centralized model with add blockchain approach, highlighting how cryptographic private keys, smart contracts, and tamper-proof ledgers can mitigate phishing, brute-force attacks, and single points of failure. Current data from 2017– 2025 is integrated to underscore challenges like rising cyber incidents and password fatigue among Indian users.

Date of Submission: 20-04-2025 Date of acceptance: 02-05-2025

I. Introduction

Cybersecurity has become a critical concern for educational institutions, especially in India's rapidity's, colleges, and schools now hold vast troves of sensitive data – personal student information, academic records, research outputs – making them prime targets for cybercriminals. Unfortunately, the rise in digital adoption has been accompanied by a sharp increase in cyber-attacks on the education sector. Recent studies show that Indian educational organizations face an average of **8,195 cyber-attacks per week**, more than double the global average of 3,355, largely due to expanded online learning and digitization during the COVID- 19 pandemic (Cyber attacks surge in education institutions across country, 8,000+ weekly incidents reported: Report - Times of India) (Cyber-attacks surge in education institutions across country, 8,000+ weekly incidents reported: Report - Times of India). This surge underscores the urgent need for stronger security measures to protect sensitive data from escalating threats.

Traditional username-password authentication systems are proving inadequate against modern attacks. Users often choose weak passwords or reuse them across platforms, making it easier for attackers to compromise accounts. Data breaches frequently expose millions of credentials; in many cases, stolen or brute-forced passwords are the gateway for attackers. In fact, over **80% of hacking-related breaches** involve lost or stolen credentials or brute force attacks (Unpacking 2020's Verizon DBIR - Human Error and Greed Collide | Duo Security). In India, incidents of large-scale credential leaks have made headlines. For example, in 2018 the personal details (phone numbers, email IDs, addresses) of **2.4 lakh** students who took the NEET medical entrance exam were found being sold online after attackers accessed a central database (Data of 2.4 lakh NEET candidates leaked and available for sale: Report - MEDIANAMA) (Data of 2.4 lakh NEET candidates leaked and available for sale: Report - MEDIANAMA). Such breaches highlight how a single compromised server or database can expeditious. The fallout is severe – identity theft, privacy violations, and erosion of trust in institutional systems.

Technical Architecture of the Blockchain-Based Security Framework

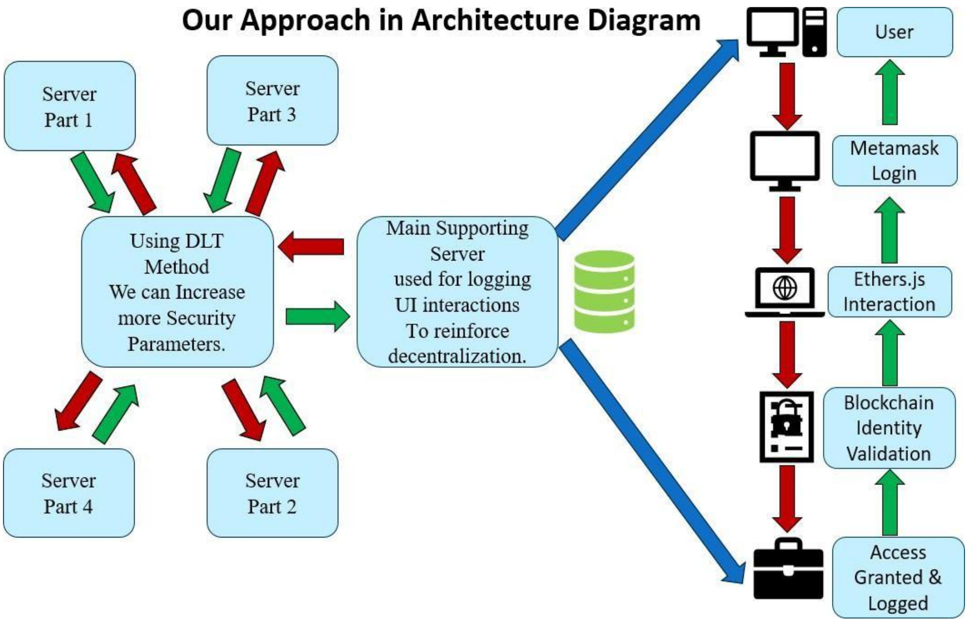
Implementing blockchain-based login in practice involves a combination of frontend and backend components working together, with the blockchain at the core of trust. Here we describe a high-level architecture for a **Blockchain-Based Unified Security Framework** as envisioned for an educational institution (like a university). This framework was prototyped by the “DarkNova Coders” team in a Kalinga University hackathon (2025) and draws on Ethereum blockchain technology, but the concepts could be adapted to other DLT platforms as well.

1. **User Interface (Web Frontend):** The students, faculty, or admins interact through a web portal (e.g., a university intranet or exam portal). This frontend is a typical web application (built with frameworks like React.js) but is “Web3- enabled.” This means it can connect to blockchain networks via JavaScript APIs (for instance, using a library like **Ethers.js**). When a user attempts to log in, instead of asking for a username and password, the application triggers a request to the user’s crypto wallet. In practical terms, the user would click a **“Login with Blockchain”** button. The web app then uses Ethers.js to ask the user’s wallet (e.g., MetaMask extension in their browser) to **sign a login message**. This message could be a random nonce (to avoid replay attacks) or could be a transaction that calls a login function on the smart contract.
2. **User Wallet (e.g., MetaMask):** MetaMask or similar Ethereum wallets serve as the custodian of the user’s private key. When the login request is initiated, the wallet pops up in the user’s browser, showing details of what is being signed (for example, “Login to University Portal at [time]”). The user confirms, and the wallet uses the private key to produce a **digital signature**. This signature is essentially the user proving “I possess the private key corresponding to my public address.” No password or biometric leaves the user’s machine; only the cryptographic signature (which can be verified but not forged by anyone without the private key) is returned to the web app.

3. **Blockchain Network (Ethereum or Consortium Chain):** The web app then sends the signature to the blockchain for verification. There are two possible flows:

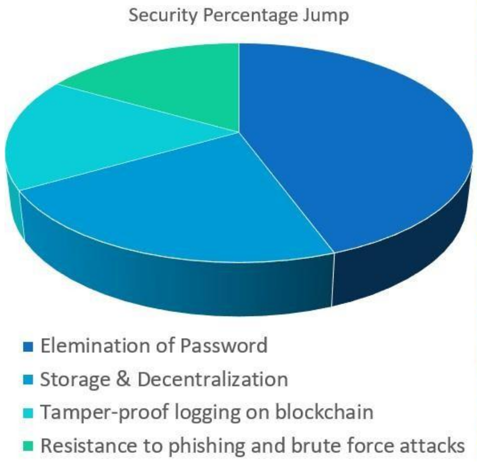
- **Off-chain signature verification:** The web server can call a view function on the smart contract (or use a library) to check the signature against the user’s public key *without* making a transaction. If valid, the contract returns true and the login proceeds. This approach doesn’t cost gas and is instant, but it requires the server to do the check (though still using on-chain data for truth).

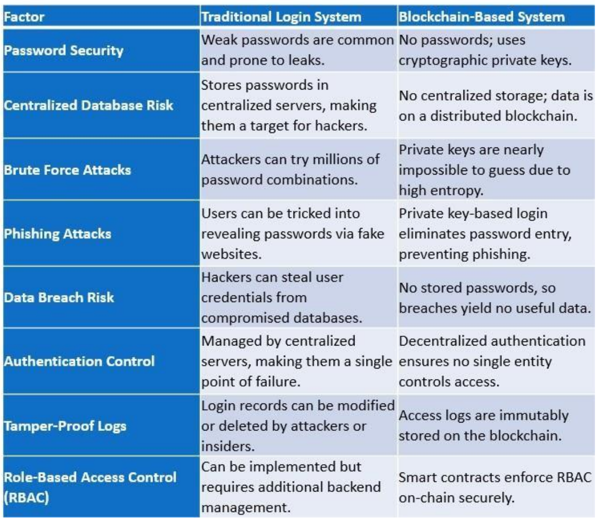
4. **Decentralized Access Control & Logging:** Upon successful authentication, the contract can emit an event, say Login Success (address user, string role, time). This event is recorded on the blockchain ledger and can be listened to by any node or even the frontend. This provides a **tamper-proof log** entry for that login. If someone attempted and failed (e.g., not in the authorized list), the contract could emit a Login Failed event or simply not emit anything (and the transaction would still be visible as a failed call). Because multiple blockchain nodes witness and record these events, no attacker can retroactively remove the evidence. This fulfils the audit trail requirement in a robust way.


Our Approach in Architecture Diagram
Server Part 1
Server Part 3
Using DLT Method We can Increase more Security Parameters.
Main Supporting Server used for logging UI interactions To reinforce decentralization.
Server Part 4
Server Part 2
User
Metamask Login
Ethers.js Interaction
Blockchain Identity Validation
Access Granted & Logged

At this point, the user is considered authenticated. However, constantly querying the blockchain for each page request is inefficient. So typically:The web server (or the frontend) will issue a short-lived **session token** (like a JWT – JSON Web Token) after it sees the on- chain authentication. This token might include the user's public address and role and be signed by the server for the client to use subsequently. The client can then use this token to make regular API requests for a limited time, avoiding hitting the blockchain for every action. The key difference is that the **initial trust** was established via blockchain verification instead of a password check.

Traditional VS Blockchain Login System





Factor	Traditional Login System	Blockchain-Based System
Password Security	Weak passwords are common and prone to leaks.	No passwords; uses cryptographic private keys.
Centralized Database Risk	Stores passwords in centralized servers, making them a target for hackers.	No centralized storage; data is on a distributed blockchain.
Brute Force Attacks	Attackers can try millions of password combinations.	Private keys are nearly impossible to guess due to high entropy.
Phishing Attacks	Users can be tricked into revealing passwords via fake websites.	Private key-based login eliminates password entry, preventing phishing.
Data Breach Risk	Hackers can steal user credentials from compromised databases.	No stored passwords, so breaches yield no useful data.
Authentication Control	Managed by centralized servers, making them a single point of failure.	Decentralized authentication ensures no single entity controls access.
Tamper-Proof Logs	Login records can be modified or deleted by attackers or insiders.	Access logs are immutably stored on the blockchain.
Role-Based Access Control (RBAC)	Can be implemented but requires additional backend management.	Smart contracts enforce RBAC on-chain securely.

Future Scope and Enhancements

The field of decentralized identity and blockchain security is rapidly evolving. Many of the current limitations can be mitigated over time through technological advances and refined approaches. Here are several **future enhancements and directions** that could improve or extend the blockchain-based authentication framework:

1. **Biometric Integration for Key Management:** One promising avenue is combining biometrics with blockchain wallets to improve usability. Modern smartphones and laptops have fingerprint readers or facial recognition. Instead of the user remembering a password or even a PIN for their wallet, the device could lock/unlock the private key using the users biometric. For example, Alice's private key is stored in her phone's secure enclave; when she tries to log in, she just uses her fingerprint on the phone, which then releases the key for signing. This makes the process seamless – effectively "Login with Fingerprint" but underlying it is "Fingerprint unlocks blockchain key which logs in." It addresses the key management issue by tying the key to something the user inherently has (their biometrics). Importantly, the biometric data itself is not stored on the blockchain (that would be a privacy disaster); it remains local to the device. As many Indian services (like phone banking, Aadhaar- based verification, etc.) have acclimatized users to fingerprint or face scans, this could be an acceptable method. In fact, India's Aadhaar uses biometrics for identity proof, so people are familiar with the concept of "my fingerprint = access." In our case it would be, "fingerprint unlocks your digital identity wallet." This could eliminate the need to remember seed phrases in daily usage – users would only need those if they change devices. Companies and projects are already working on such biometric secured wallets, and some laptops (like Windows Hello or Apple's Touch ID with Secure Enclave) effectively support this usage.

2. **Multi-Chain and Interoperability Solutions:** Right now, we might use one particular blockchain network. In the future, systems might leverage multiple networks optimally. For example, an institution could accept logins via Ethereum, Polygon, or a government blockchain – essentially being chain-agnostic. Users might choose to use one network or another (perhaps based on what they already have). Another aspect is resilience: if one network is down or congested, the system could failover to another. Multi-chain authentication could involve checking multiple ledgers for credentials or having credentials mirrored. Interoperability protocols and bridges could sync credentials between, say, a campus blockchain and a national academic blockchain. This prevents vendor or platform lock-in and adds robustness. The hackathon team did mention "Multi- Chain Authentication" as a future concept. One scenario: University has its private chain but also registers student DIDs on a public network – if the private chain goes offline, the public one can be used to verify identity in the interim. Standards like DID are actually blockchain-neutral (a DID can have different "methods" corresponding to different chains). So, moving to a DID approach inherently allows multi-chain presence of the identity.

II. Conclusion

Blockchain-based authentication is poised to be a **game-changer** for secure access management in educational institutions and beyond. This comprehensive analysis showed how a decentralized, DLT-driven framework can address the pressing challenges of cybersecurity in India's education sector, providing a safer and more efficient alternative to traditional password systems.

Traditional login systems, with their reliance on human-chosen passwords and centralized databases, have proven inadequate in the face of rising cyber threats. Indian educational institutions, in particular, are facing an onslaught of attacks – **twice as many attacks on average** compared to global figures – exposing how vulnerable the status quo is. We saw how major breaches, like the NEET data leak affecting 2.4 lakh students, underscore weaknesses such as single-point failures of centralized databases. Users are often the weak link, reusing passwords and falling for phishing, while institutions struggle to secure sprawling systems with limited resources.

A blockchain-based unified framework fundamentally flips the security model to be **"trust less, decentralized, and secure."** By using cryptographic keys instead of passwords, we remove the easiest targets (no credentials to steal in bulk, no password to phish) and greatly strengthen resistance to brute-force attacks (since 256-bit keys are practically uncrackable). The ledger, distributed across nodes, means there is no central server that, if compromised or down, can break the whole system. Instead, **every login and action is validated by code on a distributed ledger and recorded immutably**, creating inherent accountability.

We detailed how such a system works in practice: from a student using a wallet like MetaMask to log in, to a smart contract on Ethereum (or a similar network) verifying roles and logging events. We compared this to traditional methods (Table 1) and saw clear advantages in every aspect – be it eliminating credential databases that can be dumped by hackers, or ensuring that audit logs cannot be quietly tampered with by an attacker or rogue admin. The **transparency** of blockchain logs foster trust: stakeholders can independently verify activities, and forensic investigations have reliable data.

References

[1]. **DarkNova Coders.** "Kalinga University Hackathon 2025 – Blockchain Based Unified Security Framework" – Project Presentation Excerpts (2025). Excerpts highlighting the introduction of blockchain authentication benefits, advantages (phishing resistance, tamper-proof logs, no centralized password store), as well as limitations (internet dependence, key management) and future enhancements (biometric login, multi-chain, DID, ZKP integration) from a student project presentation. [Referencing insights on the proposed framework's features and envisioned improvements].

[2]. **Check Point Software (cited in Times of India).** "Cyber-attacks surge in education institutions across country, 8,000+ weekly incidents reported: Report" (Sep 29, 2024). Reveals that Indian education sector organizations face ~8,195 cyberattacks per week vs. global average of ~3,355, attributed to remote learning during COVID-19. Mentions other sectors for comparison (healthcare 7,982; govt/military 4,590 per week) and includes a quote from Sundar Balasubramanian (Check Point India MD) about targeting of PII in critical sectors.

[3]. **Media Nama.** "CERT-In handled nearly 14 lakh cyber incidents in 2022" – Sarvesh M. (Nov 22, 2023). Cites an official figure of 13,91,457 cybersecurity incidents reported to CERT-In in 2022 (as per IT Ministry's response in Parliament), and discusses the low compliance with the 6-hour incident reporting rule. Indicates the scale of incidents and challenges in incident response.

[4]. **Times of India.** "More than 6.07 lakh cyber security cases reported till June 2021: Union minister tells Parliament" (Jul 29, 2021). Reports CERT-In statistics: 3,94,499 incidents in 2019; 11,58,208 in 2020; and 6,07,220 in the first half of 2021. Shows the surge during the pandemic. Includes statement by MoS IT Rajeev Chandrasekhar and notes measures taken by the government.

[5]. **Media Nama.** "Data of 2.4 lakh NEET candidates leaked and available for sale: Report" – Trisha Jalan (July 19, 2018). Details a breach where personal data (phone, email, address) of 240,000 students who took the NEET medical exam was found being sold online for Rs 2 lakh. Data spanned 15 states. Highlights risk of centralized exam databases and mentions a similar breach in 2017 of MBA entrance exam data.