Prantik Gabeshana Patrika
Multidisciplinary-Multilingual
Peer Reviewed (Double Blind Referred)
Bi-Annual Research e-Journal

Volume-5 Issue-1 July 2026
International e-ISSN 2583-6706
Website
santiniketansahityapath.org.in

INDEXED IN INTERNET ARCHIVE | GOOGLE SCHOLAR | ORCID | SCRIBD | ACADEMIA

DOI https://doi.org/10.67841/pgp.260501073 OPEN ACCESS

IIFS Impact Factor 3.75 SJIF Impact Factor 3.481

The Evolution of Blockchain Technology and the Security of Social Data: A Research Concept and Analysis
ব্লকচেইন প্রযুক্তির উদ্ভব ও সামাজিক ডেটার নিরাপত্তা: একটি গবেষণামূলক ধারণা এবং বিশ্লেষণ

Dr. Ashis Kumar Samanta
Database Administrator
Calcutta University

Received on: 02nd June 2026
Accepted on: 12th June 2026

Abstract:
In the current digital era, information security has become a critical issue. Safeguarding personal, financial, and business data — which is frequently exchanged online — poses a significant challenge. Blockchain technology has brought about a revolutionary shift in this landscape, emerging as an effective method for ensuring data security. Blockchain is a form of Distributed Ledger Technology (DLT) in which data is stored in blocks, with each block interconnected via cryptography. Each block contains specific data, a timestamp, and the hash of the preceding block. This structure makes it extremely difficult to alter or tamper with the data. This article evaluates blockchain technology and demonstrates its application in securing transaction-related data, thereby fostering public trust in the information and enabling error-free decision-making.

Key Words:
Blockchain, data security, distributed networks, cryptography.

মূল প্রবন্ধ

১.ভূমিকা

অনলাইন অ্যাপ্লিকেশনের জন্য ডেটা সংরক্ষণের জন্য ক্লাউডের ব্যবহার একটি জনপ্রিয় প্রযুক্তি হয়ে উঠেছে। এটি পরবর্তী প্রজন্মের একটি দৃষ্টান্ত হয়ে উঠেছে। স্মার্টফোনের ব্যাপক ব্যবহার এবং ফেসবুক, হোয়াটস্অ্যাপ ইত্যাদির মতো জনপ্রিয় অ্যাপ্লিকেশনের সঙ্গে, ব্যক্তিরা এটি না বুঝেও ক্লাউড স্টোরেজ ব্যবহারে আরো অভ্যস্ত হয়ে উঠেছে। তবে, ব্যবহারকারী এবং ক্লাউড প্রদানকারী নির্বিশেষে, ক্লাউডে ডেটার নিরাপত্তা এখনো একটি বড়ো সমস্যা। ডেটা নিরাপত্তা, গোপনীয়তা এবং ক্লাউড-ভিত্তিক অ্যাপ্লিকেশনগুলিতে ডেটা স্বচ্ছতা অর্জনের জন্য বিভিন্ন ক্ষেত্রে অ্যাপ্লিকেশনগুলি বাস্তবায়িত হয়। ব্লকচেইন ফ্রেমওয়ার্কে চালিত স্মার্ট কন্ট্রাক্টগুলির মূল্যায়ন আজকাল বিভিন্ন ব্যবসায়িক খাতে ডেটা নিরাপত্তা অর্জনের জন্য ব্যবহৃত হয়। তবে, বাস্তব জীবনে বাস্তবায়নের ক্ষেত্রে দেখা যায় যে ব্লকচেইন নিজেই বিভিন্ন নিরাপত্তা হুমকির সম্মুখীন হচ্ছে।

ইন্টারনেটের মাধ্যমে অ্যাপ্লিকেশন সমর্থন এবং অবকাঠামোগত সমর্থন, কম খরচে এবং হ্যান্ডলিং ঝুঁকি হ্রাসের সঙ্গে, মানুষকে বিতরণকৃত পরিবেশে ডেটা এবং ব্যবসা অন্বেষণে আকর্ষণ করে যা ক্লাউড কম্পিউটিং পরিবেশের সুবিধা। ক্লাউডের পরিষেবা সমর্থন চাহিদার ভিত্তিতে ক্লাউড গ্রাহকদের প্রদান করা হয়। ক্লাউড নিয়ন্ত্রণ বিভিন্ন বিক্রেতার মধ্যে ভাগ করা হয়; তাই, ক্লাউড ডেটা সর্বদা উচ্চ ঝুঁকিতে থাকে। ক্লাউড ডেটা সুরক্ষিত করার জন্য ক্রিপ্টোগ্রাফি এবং ক্লাউড-সক্ষম প্রযুক্তি বিশ্বে প্রবর্তিত হয়েছিল। ব্লকচেইন ইতিমধ্যেই

© Santiniketan Sahityapath

অনলাইন লেনদেন এবং দৈনন্দিন অ্যাপ্লিকেশনের বিভিন্ন ক্ষেত্রে তার গবেষণার ডানা প্রসারিত করেছে। এটি একটি বিতরণকৃত, পিয়ার-টু-পিয়ার, ট্যাম্পারপ্রুফ, ক্রিপ্টোগ্রাফি-ভিত্তিক প্রযুক্তি।

নেটওয়ার্ক প্রতিটি লেনদেনের জন্য একটি হ্যাশ কী বজায় রাখে। যদিও ডেটা পাবলিক নেটওয়ার্কে বিতরণের প্রাথমিক ধারণা ছিল, অ্যাপ্লিকেশনের প্রয়োজনীয়তার কারণে, ব্যক্তিগত এবং কনসোর্টিয়ামও অনেক অ্যাপ্লিকেশনে অন্তর্ভুক্ত করা হয়েছে এবং ডেটা লেনদেন সুরক্ষিত করার জন্য অনেকগুলি কনসেনসাস অ্যালগরিদম ব্যবহৃত হয়। যদিও এটির রিয়েল-টাইম অ্যাপ্লিকেশন তৈরির অনেক সম্ভাবনা রয়েছে, তবুও এটির কিছু সীমাবদ্ধতা রয়েছে কারণ এটি এখনো গবেষণা এবং উন্নয়নের প্রাথমিক পর্যায়ে রয়েছে।

ব্লকচেইন প্রযুক্তি (বিসিটি) হলো একটি বিকেন্দ্রীভূত, পিয়ার-টু-পিয়ার (পি-টু -পি) নেটওয়ার্ক যা একটি ডিস্ট্রিবিউটেড লেজার হিসেবে কাজ করে। প্রাথমিকভাবে বিটকয়েনের মতো ডিজিটাল মুদ্রার সঙ্গে এটি প্রবর্তিত হলেও, বিসিটির প্রভাব ব্যাংকিং, স্বাস্থ্যসেবা, এবং সরকার-সহ বিভিন্ন ক্ষেত্রে প্রসারিত হয়েছে। এর মূলে, বিসিটি হলো ধারাবাহিক লেনদেনের ব্লকগুলির একটি ক্রমাগত বর্ধনশীল চেইন। প্রথাগত সিস্টেমের বিপরীতে, এটি বিকেন্দ্রীভূত যা প্রতিটি অংশগ্রহণকারীকে নেটওয়ার্ক নিয়ন্ত্রণ করতে দেয়। নেটওয়ার্কের কম্পিউটারগুলিকে নোড বলা হয় এবং প্রতিটি নোডের কাছে ডিজিটাল লেজারের একটি কপি থাকে। ব্লকগুলি হলো ডেটা ধারণকারী পাত্র যা লেনদেনের বিবরণ, একটি টাইমস্টাম্প এবং ক্রিপ্টোগ্রাফিক ফাংশন ও পয়েন্টারের মাধ্যমে পূর্ববর্তী ব্লকের একটি লিঙ্ক সংরক্ষণ করে একটি রৈখিক চেইন গঠন করে।

একটি গুরুত্বপূর্ণ বৈশিষ্ট্য হলো সমগ্র নেটওয়ার্কের ঐকমত্য ছাড়া একটি ব্লক পরিবর্তন করা যায় না। নতুন ব্লক যাচাই করার জন্য নির্দিষ্ট প্রোটোকল এবং প্রতিটি অংশগ্রহণকারীর চুক্তি প্রয়োজন। বিসিটি সংজ্ঞায়িত হয় ঐকমত্য (consensus), ডিস্ট্রিবিউটেড কম্পিউটেশন, অপরিবর্তনীয়তা (immutability — স্থায়ী রেকর্ড), এবং প্রমাণীকরণ (authentication) দ্বারা। এর বিকাশমান প্রকৃতির কারণে, বিভিন্ন অ্যাপ্লিকেশন বিভিন্ন ধরণের ব্লকচেইন ব্যবহার করে: পারমিশনলেস (পাবলিক) যেখানে যে কেউ অংশগ্রহণ করতে পারে; পারমিশনড যা অনুমোদিত ব্যবহারকারীদের জন্য সীমাবদ্ধ থাকে এবং ব্লকগুলি এনক্রিপ্ট করা হয়; এবং কনসোর্টিয়াম, যা একটি হাইব্রিড। কার্যপ্রণালীতে একজন পক্ষ একটি লেনদেন শুরু করে একটি ব্লক তৈরি করে। নেটওয়ার্কের কম্পিউটারগুলি এই ব্লকটি যাচাই করে, এরপর এটি চেইনে যুক্ত করা হয় এবং নেটওয়ার্ক জুড়ে সংরক্ষিত হয়। এর সম্ভাবনা সত্ত্বেও, বিসিটি বেশ কয়েকটি চ্যালেঞ্জের সম্মুখীন হয়, যার মধ্যে রয়েছে দক্ষতার প্রয়োজনীয়তা, অবকাঠামোর জন্য উল্লেখযোগ্য প্রাথমিক খরচ, গোপনীয়তা ও নিরাপত্তা সংক্রান্ত উদ্বেগ, স্কেলেবিলিটির সমস্যা, এবং আইনি নিয়মকানুন।

২. বিভিন্ন ধরনের সাইবার নিরাপত্তা বিষয়ক আক্রমণ

ডেটা সর্বদা অভ্যন্তরীণ এবং বাহ্যিক হুমকির মুখে থাকে। কিছু আক্রমণ যা ডেটাকে আরো ঝুঁকিপূর্ণ করে তা নীচে উল্লেখ করা হয়েছে (Sinha et al., 2019)।

ডিনায়াল-অফ-সার্ভিস (DoS): এই আক্রমণ সিস্টেমের সম্পদ অতিরিক্ত ব্যবহার করে সেবা প্রদানে বাধা দেয়। ডিস্ট্রিবিউটেড ডিনায়াল-অফ-সার্ভিস (DDoS) আক্রমণও একইভাবে সম্পদ নিঃশেষ করে, তবে এটি ম্যালওয়্যার-আক্রান্ত অনেক মেশিন দ্বারা পরিচালিত হয়। DoS আক্রমণে সাইট অবৈধ অনুরোধে প্লাবিত হয় যা সাইটের সম্পদ হ্রাস করে এবং স্বাভাবিক সেবা প্রদানে বাধা দেয়, প্রায়ই সাইট সম্পূর্ণ বন্ধ করে দেয়।

ফিশিং আক্রমণ: এই আক্রমণ হলো যখন দুর্বৃত্তরা বিশ্বস্ত উৎস থেকে আসা মনে হয় এমন ইমেল পাঠায়, সংবেদনশীল তথ্য চুরির জন্য। এটি সামাজিক প্রকৌশল ও প্রযুক্তির সমন্বয়। আক্রমণকারী লিঙ্ক পাঠায় যা ম্যালওয়্যার ডাউনলোড বা ব্যক্তিগত তথ্য প্রকাশ করায়। প্রায়শই, শিকার বুঝতে পারে না তারা আক্রান্ত, ফলে আক্রমণকারী সংস্থার অন্যদের লক্ষ করে, কেউ সন্দেহ না করে।

র‍্যানসমওয়্যার আক্রমণ: এই আক্রমণে, শিকারের সিস্টেম বন্দী থাকে যতক্ষণ না তারা আক্রমণকারীকে মুক্তিপণ দেয়। পেমেন্টের পর, আক্রমণকারী নিয়ন্ত্রণ ফিরিয়ে নেওয়ার নির্দেশ দেয়। শিকার ওয়েবসাইট বা ইমেল সংযুক্তি থেকে র‍্যানসমওয়্যার ডাউনলোড করে। এটি

© Santiniketan Sahityapath

সিস্টেমের দুর্বলতা শোষণ করে, ওয়ার্কস্টেশন এনক্রিপ্ট করে। কখনো কখনো, এটি একাধিক কম্পিউটার বা সার্ভারে আঘাত করে, নেটওয়ার্ক বা ইউএসবি'র মাধ্যমে ছড়িয়ে।

SQL ইনজেকশন আক্রমণ: SQL ইনজেকশন হলো ওয়েবসাইটের ডাটাবেসের দুর্বলতা কাজে লাগানোর একটি পদ্ধতি। ক্লায়েন্ট থেকে সার্ভারের ডাটাবেসে ক্ষতিকর এসকিউএল কোয়েরি পাঠানো হয় যা পাসওয়ার্ড বা লগইনের জায়গায় ঢোকানো হয়। সফল হলে, সংবেদনশীল তথ্য ফাঁস, ডাটা মুছে ফেলা বা সিস্টেম বন্ধ হতে পারে। সুরক্ষার জন্য, ন্যূনতম-অধিকার মডেল ব্যবহার করুন, যেখানে শুধু প্রয়োজনীয় ব্যক্তিরাই ডাটাবেসে প্রবেশ করতে পারেন।

চিত্র ১: সাইবার হুমকির ল্যান্ডস্কেপ

সেশন হাইজ্যাকিং: এই আক্রমণে হলো একটি MITM আক্রমণ, যেখানে আক্রমণকারী ক্লায়েন্ট ও সার্ভারের মধ্যে সেশন নিয়ন্ত্রণ করে। আক্রমণকারীর কম্পিউটার ক্লায়েন্টের আইপি অ্যাড্রেস প্রতিস্থাপন করে, এবং সার্ভার সেশন চালিয়ে যায়, ভেবে যে এটি ক্লায়েন্টের সঙ্গে যোগাযোগ করছে। সার্ভার ক্লায়েন্টের আইপি দিয়ে পরিচয় যাচাই করে, তাই মাঝপথে আক্রমণকারীর আইপি ঢুকলে সন্দেহ হয় না।

ট্রোজান হর্স আক্রমণ: এই আক্রমণে ক্ষতিকর প্রোগ্রাম নিরীহ প্রোগ্রামের ভিতর লুকানো থাকে। ব্যবহারকারী এটি চালালে, ম্যালওয়্যার সিস্টেমে ব্যাকডোর খোলে যার মাধ্যমে হ্যাকাররা কম্পিউটার বা নেটওয়ার্কে প্রবেশ করে।

ম্যালওয়্যার আক্রমণ: ম্যালওয়্যার হলো ক্ষতিকর সফটওয়্যার যা কম্পিউটারে সংক্রমিত হয়ে এর কার্যকারিতা পরিবর্তন করে, ডাটা নষ্ট করে বা গুপ্তচরবৃত্তি করে। এটি ডিভাইসে ছড়াতে পারে বা শুধু হোস্টকে প্রভাবিত করে। ফায়ারওয়াল ও সতর্কতা জরুরি।

ব্রুট ফোর্স আক্রমণ: এই আক্রমণে আক্রমণকারী সিস্টেমে প্রবেশের জন্য লগইন ক্রেডেনশিয়াল অনুমান করে। বট ব্যবহার করে তারা সম্ভাব্য ক্রেডেনশিয়ালের তালিকা পরীক্ষা করে। সঠিক ক্রেডেনশিয়াল পেলে প্রবেশ সম্ভব। লক-আউট নীতি, যেমন কয়েকটি ভুল চেষ্টায় অ্যাকাউন্ট ফ্রিজ, এটি প্রতিরোধ করে।

ডিএনএস স্পুফিং আক্রমণ: এই আক্রমণে হ্যাকার ডিএনএস রেকর্ড পরিবর্তন করে ট্রাফিক ভুয়ো ওয়েবসাইটে পাঠায়। শিকার সেখানে সংবেদনশীল তথ্য প্রবেশ করায় যা হ্যাকার ব্যবহার বা বিক্রি করে। হ্যাকার প্রতিযোগী কোম্পানির মানহানির জন্য নিম্নমানের সাইটও তৈরি করতে পারে।

© Santiniketan Sahityapath

৩. গবেষণার উদ্দেশ্য

বিশ্বজুড়ে সব ক্ষেত্রে একটি ডিজিটাল বিস্ফোরণ ঘটছে এবং তারপরে বেশিরভাগ অ্যাপ্লিকেশনই অনলাইন হয়ে গেছে, কারণ সমাজ অনলাইন লেনদেনের সঙ্গে অভ্যস্ত হয়ে পড়েছে, অন্যান্য প্রকৃত বা বাস্তব লেনদেনের ধরণের পরিবর্তে যা বিপুল পরিমাণে উৎপন্ন হচ্ছে এবং এই বিপুল পরিমাণ ডেটার সঙ্গে এখন এটি সবই বিগ ডেটা। এখন এই বিগ ডেটার নিরাপত্তা নিয়ে প্রশ্ন ওঠে কারণ সমাজকে এই ডেটার উপর ভরসা করতে হয় যতক্ষণ না সেই ডেটা নিরাপদ এবং সমাজের কাছে বিশ্বস্ত হয়, ততক্ষণ সঠিক সিদ্ধান্ত নেওয়া যায় না। সমাজ সামগ্রিকভাবে এই ডেটার উপর খুব নির্ভরশীল হয়ে পড়েছে। অতএব, নিবন্ধের উদ্দেশ্য হলো এই বিগ ডেটার নিরাপত্তার বিষয়টি সমাধান করা, এবং যদি ডেটা নিরাপদ হয়, তবে এটি সমাজের জন্য ডেটার প্রকৃত লক্ষ অর্জন করবে।

৪. প্রাসঙ্গিক সাহিত্য পর্যালোচনা

এম. ঝু এবং অন্যান্যরা মহাকাশ তথ্য নেটওয়ার্কের জন্য একটি বিশ্বস্ত সুরক্ষা পদ্ধতি প্রস্তাব করেছেন, যা টিপিএম (trusted platform module), এসজিএক্স-ভিত্তিক টিইই (trusted execution environment) এবং গুণাবলি-ভিত্তিক অ্যাক্সেস নিয়ন্ত্রণকে একীভূত করে সংবেদনশীল ডেটা সুরক্ষিত করে। এই কাঠামো অভ্যন্তরীণ ও বাহ্যিক হুমকি থেকে অননুমোদিত অ্যাক্সেস, পরিবর্তন এবং ফাঁস প্রতিরোধ করে, নিরাপদ ডেটা সংক্রমণ এবং সূক্ষ্ম অ্যাক্সেস নিয়ন্ত্রণ নিশ্চিত করে (Zhu & Wang, 2025)। এল. পিং এবং অন্যান্যরা ইআইএস-এর জন্য বিগ ডেটা-ভিত্তিক ঝুঁকি ভবিষ্যদ্বাণী মডেল প্রস্তাব করেছেন যা ডেটা মাইনিংয়ের মাধ্যমে হুমকি সনাক্তকরণ উন্নত করে। এটি AUC-তে ঐতিহ্যগত পদ্ধতিকে ছাড়িয়ে যায়, BDT ব্যবহার করে প্রাথমিক সতর্কতা, অসঙ্গতি সনাক্তকরণ এবং ঝুঁকি পরিমাপে সহায়তা করে। অপ্টিমাইজড প্যারামিটার এবং ফিচার ইঞ্জিনিয়ারিং কর্মক্ষমতা বাড়ায়, উদ্যোগের প্রতিক্রিয়া ও সিদ্ধান্ত গ্রহণ উন্নত করে। ভবিষ্যতে শিল্প-নির্দিষ্ট মডেল এবং গ্রাফ নিউরাল নেটওয়ার্কের মতো DL প্রযুক্তি একীকরণ সম্ভব (Li & Zhang, 2025)।

এম. এ. পোল্টাভৎসেভা বিগ ডেটা সিস্টেমের সুরক্ষা মূল্যায়নের নতুন পদ্ধতি প্রস্তাব করেছেন যা অ্যাক্সেস নিয়ন্ত্রণ এবং বিশেষাধিকারপ্রাপ্ত ব্যবহারকারীদের বিবেচনা করে। এটি গাণিতিকভাবে মূল্যায়নকে আনুষ্ঠানিক করে, বাস্তবায়নের পর্যায় বর্ণনা করে এবং একটি পরীক্ষামূলক উদাহরণ উপস্থাপন করে, বিদ্যমান আইএস সুরক্ষা পদ্ধতির উন্নতি করে (Poltavtseva et al., 2024)। এক্স. চেইন এবং অন্যান্যরা ইথেরিয়ামের বীকন চেইনের সুরক্ষা হুমকি সনাক্তকরণের জন্য প্রথম ভিজ্যুয়াল অ্যানালিটিক টুল প্রস্তাব করেছেন। বিশেষজ্ঞদের সঙ্গে সহযোগিতায়, এটি তিনটি ইন্টারেক্টিভ ভিউ অফার করে যা ঐতিহাসিক ব্লকগুলিতে দুর্বলতা চিহ্নিত করে, কেস স্টাডির মাধ্যমে প্রকৃত ঘটনাগুলির বিস্তারিত তদন্ত প্রদর্শন করে (Chen et al., 2024)। বি. হুয়া এবং অন্যান্যরা ক্যাওটিক সিস্টেম-ভিত্তিক চিত্র এনক্রিপশন অ্যালগরিদম ব্যবহার করে বিগ ডেটা (বিডি) সুরক্ষা ও গোপনীয়তা সুরক্ষা মডেল প্রস্তাব করেছেন। এটি ঐতিহ্যগত মডেলের তুলনায় উৎকৃষ্ট, ডেটা গোপনীয়তা ও অনুপ্রবেশ আক্রমণের বিরুদ্ধে উন্নত সুরক্ষা প্রদান করে। মডেলটি পিক্সেল সম্পর্ক হ্রাস করে এনক্রিপশন উন্নত করে। পরীক্ষায় টুপল (৮২.২৫%), গুণাবলি (৮২.৪১%), এবং সম্ভাব্য (৮১.৯৭%) আক্রমণের বিরুদ্ধে ঐতিহ্যগত মডেলের (৭৫.১৫%, ৭৭.২৬%, ৭৬.৩৮%) তুলনায় উচ্চতর সুরক্ষা হার দেখায়, এর উৎকৃষ্ট কার্যকারিতা প্রমাণ করে এবং ভবিষ্যত বিডি সুরক্ষার দিকনির্দেশনা প্রদান করে (Hua et al., 2023)।

এ. এ. ফার্সির পেপার ইউএভি ইকোসিস্টেমে ফেডারেটেড লার্নিং (এফএল) পর্যালোচনা করে, গোপনীয়তা ও সুরক্ষা উদ্বেগ সমাধানে এর ভূমিকার উপর জোর দেয়। এফএল-এর বিকেন্দ্রীকৃত পদ্ধতি ডেটা সংক্রমণ হ্রাস করে গোপনীয়তা বাড়ায়। গবেষণায় সুরক্ষা চ্যালেঞ্জ, সুরক্ষিত সমষ্টি ও হালকা ক্রিপ্টোগ্রাফির মতো প্রতিরক্ষা পদ্ধতি প্রস্তাব করা হয় এবং গবেষণার ফাঁক চিহ্নিত করা হয়। এটি নিরাপদ, নৈতিক এফএল-ভিত্তিক ইউএভি স্থাপনার জন্য বাস্তব-বিশ্বের বৈধতা ও নিয়ন্ত্রণ কাঠামোর পক্ষে সমর্থন করে (Farsi et al., 2025)। ওয়াই. ঝাং-এর নিবন্ধে UWBAD+ উপস্থাপন করা হয়েছে, একটি DoS আক্রমণ যা রিঅ্যাকটিভ জ্যামিং ব্যবহার করে বাণিজ্যিক আল্ট্রা-ওয়াইডব্যান্ড (UWB) রেঞ্জিং সিস্টেমকে বিঘ্নিত করে। নরমালাইজড ক্রস-কোরিলেশনের দুর্বলতা কাজে লাগিয়ে, UWBAD+ পূর্বের ডিভাইস জ্ঞান ছাড়াই রেঞ্জিং সেশন বন্ধ করে, সম্পত্তি হ্রাস বা অননুমোদিত অ্যাক্সেসের ঝুঁকি তৈরি করে। এর কম সনাক্তযোগ্যতা ও সাশ্রয়ী মূল্য দ্রুত স্নিফিং, ফিল্ড-লেভেল জ্যামিং এবং COTS UWB চিপ থেকে আসে। অ্যাপল, এনএক্সপি, এবং কোরভো সিস্টেমে সফল আক্রমণের পর, একটি OEM দুর্বলতা স্বীকার করে $৫,০০০ বাউন্টি প্রদান করেছে (Zhang et al.,

© Santiniketan Sahityapath

2025)। এস. ঘোষের পেপার প্রস্তাব করে, যা ব্যাখ্যাযোগ্য XAI-RNN-SGRU-কে (ইক্স্প্লেনবল AI, রিজলেট নিউরাল নেটওয়ার্ক এবং সফট গেটেড রিকারেন্ট ইউনিট) একত্রিত করে সাইবার নিরাপত্তা ও আর্থিক ডেটা ভবিষ্যদ্বাণী উন্নত করে। উন্নত প্রিপ্রসেসিং, EPCA (Enhanced Principal Component Analysis), AAO (Aphid Ant Optimization) এবং উন্নত হোমোমরফিক এনক্রিপশন ব্যবহার করে, এটি ডেটাসেট জুড়ে ৯৯.৫৫-৯৯.৯৯ % নির্ভুলতা অর্জন করে, ০.০০০০৪ বিট ত্রুটি হার এবং ৯৮.০৩ % ডেটা সুরক্ষা-সহ। এটি আর্থিক প্রতিষ্ঠানের জন্য স্কেলযোগ্য, নিরাপদ সমাধান প্রদান করে, জালিয়াতি সনাক্তকরণ, ডেটা সুরক্ষা এবং এনক্রিপশন দক্ষতায় বিদ্যমান পদ্ধতিকে ছাড়িয়ে যায় (Ghosh, 2025)।

এ. কে. সামন্ত এবং অন্যান্যরা বিশ্ববিদ্যালয় পরীক্ষা ব্যবস্থার অখণ্ডতা বাড়াতে একটি ব্লকচেইন ফ্রেমওয়ার্ক প্রস্তাব করে। এটি খালি উত্তরপত্র বিতরণ থেকে পরীক্ষা কেন্দ্রে, উত্তরপত্র মূল্যায়ন, স্কোর সংকলন এবং সার্টিফিকেট স্বয়ংক্রিয়ভাবে তৈরি পর্যন্ত নিরাপদ, অপরিবর্তনীয় প্রক্রিয়া নিশ্চিত করে। ব্লকচেইনের অপরিবর্তনীয়, এনক্রিপ্টেড লেনদেন স্কোর ম্যানিপুলেশন এবং সার্টিফিকেট জালিয়াতি প্রতিরোধ করে। একটি কেস স্টাডি হ্যাশ-ডাইজেস্ট ব্যবহার করে প্রতিটি লেনদেন পর্যায় ট্র্যাক করে ফ্রেমওয়ার্ক যাচাই করে, উত্তরপত্র, মূল্যায়ন এবং স্কোরের ট্রেসেবিলিটি সক্ষম করে। এটি পরীক্ষা প্রক্রিয়া এবং সার্টিফিকেটের প্রামাণ্যতায় বিশ্বাস বাড়ায়, ঐতিহ্যগত সিস্টেমের অসঙ্গতি দূর করে এবং শিক্ষা প্রতিষ্ঠানের জন্য স্কেলযোগ্য, নিরাপদ সমাধান প্রদান করে (Samanta & Sarkar, 2021)। এ. কে. সামন্তর গবেষণাপত্রে সাপ্লাই চেইন ম্যানেজমেন্ট (SCM) এ ব্লকচেইন প্রযুক্তি সংযোজন করে ডাটা টেম্পারিং, স্বচ্ছতা ও সিদ্ধান্ত গ্রহণের সমস্যা সমাধানের প্রস্তাব করা হয়েছে। চালের সাপ্লাই চেইনের একটি কেস স্টাডির মাধ্যমে দেখানো হয়েছে কীভাবে ব্লকচেইনের অপরিবর্তনযোগ্য লেজার ডাটা সুরক্ষা, গুণমান নিয়ন্ত্রণ ও সঠিক সিদ্ধান্ত নিশ্চিত করে (Samanta, 2021)। এই নিবন্ধে এ.কে. সমন্ত ও সহযোগীরা ডিজিটাল যুগে ডাটা সুরক্ষা ও গোপনীয়তার প্রয়োজনীয়তা তুলে ধরেছেন, যেখানে অনলাইন লেনদেন বিপুল পরিমাণ ডেটা তৈরি করে। কেন্দ্রীভূত সিস্টেম থেকে বিকেন্দ্রীভূত প্ল্যাটফর্মে স্থানান্তরের সঙ্গে সঙ্গে সাইবিল আক্রমণের মতো নিরাপত্তা ঝুঁকি বাড়ে। ব্লকচেইন, একটি পিয়ার-টু-পিয়ার ডিস্ট্রিবিউটেড লেজার, ডাটা সুরক্ষা দিলেও সাইবিল আক্রমণের শিকার হয়। এই গবেষণায় ব্লকচেইনের প্রয়োগ বিশ্লেষণ করে সাইবিল আক্রমণ সনাক্ত ও প্রতিরোধের জন্য একটি গেম-ভিত্তিক মডেল প্রস্তাব করা হয়েছে যা বিকেন্দ্রীভূত নেটওয়ার্কে নিরাপদ লেনদেন নিশ্চিত করবে (Samanta & Chaki, 2023)।

৪.১. গবেষণার প্রধান ফলাফল (Finding)

এই গবেষণাপত্রসমূহে ডেটা সুরক্ষা, গোপনীয়তা এবং সাইবার নিরাপত্তা সংক্রান্ত বিভিন্ন আধুনিক চ্যালেঞ্জ মোকাবেলায় উদ্ভাবনী প্রযুক্তি ও পদ্ধতি প্রস্তাব করা হয়েছে। মহাকাশ যোগাযোগ থেকে শুরু করে শিক্ষা ব্যবস্থা পর্যন্ত বিস্তৃত ক্ষেত্রে নিরাপত্তা ও স্বচ্ছতা নিশ্চিত করতে ব্লকচেইন, ফেডারেটেড লার্নিং, ক্যাওটিক এনক্রিপশন এবং বিগ ডেটা অ্যানালিটিক্সের মতো প্রযুক্তিগুলির প্রয়োগ পরীক্ষা করা হয়েছে। প্রতিটি গবেষণায় প্রস্তাবিত মডেল বা কাঠামো সংশ্লিষ্ট ক্ষেত্রে উল্লেখযোগ্য উন্নতি সাধন করেছে, যা ঐতিহ্যগত পদ্ধতির সীমাবদ্ধতা কাটিয়ে উঠতে সক্ষম হয়েছে।

- মহাকাশ তথ্য নেটওয়ার্কের জন্য টিপিএম, এসজিএক্স-ভিত্তিক টিইই এবং গুণাবলি-ভিত্তিক অ্যাক্সেস নিয়ন্ত্রণের সমন্বয়ে একটি নিরাপদ কাঠামো প্রস্তাব করা হয়েছে যা অভ্যন্তরীণ ও বাহ্যিক হুমকি থেকে ডেটা সুরক্ষা নিশ্চিত করে (Zhu & Wang, 2025)।
- বিগ ডেটা-ভিত্তিক ঝুঁকি ভবিষ্যদ্বাণী মডেল (BDT) ঐতিহ্যগত পদ্ধতিকে ছাড়িয়ে গেছে, AUC স্কোরে উন্নত কর্মক্ষমতা দেখিয়েছে এবং শিল্প-নির্দিষ্ট ডিপ লার্নিং মডেলের সম্ভাবনা উন্মোচন করেছে (Li & Zhang, 2025)।
- ইথেরিয়াম বীকন চেইনের জন্য ভিজ্যুয়াল অ্যানালিটিক টুল উন্নত করা হয়েছে, যা ঐতিহাসিক ব্লক ডেটা বিশ্লেষণ করে দুর্বলতা শনাক্ত করতে সক্ষম (Chen et al., 2024) ।
- ক্যাওটিক সিস্টেম-ভিত্তিক চিত্র এনক্রিপশন অ্যালগরিদম প্রচলিত মডেলের তুলনায় ৮২ % পর্যন্ত সুরক্ষা হার অর্জন করেছে, ডেটা গোপনীয়তা ও অনুপ্রবেশ প্রতিরোধে উল্লেখযোগ্য উন্নতি দেখিয়েছে (Hua et al., 2023)।
- ফেডারেটেড লার্নিং (FL) ইউএভি ইকোসিস্টেমে ডেটা গোপনীয়তা বাড়ায়, তবে বাস্তব-বিশ্বের প্রয়োগের জন্য হালকা ক্রিপ্টোগ্রাফি ও নিয়ন্ত্রণ কাঠামোর প্রয়োজন (Farsi et al., 2025) ।

© Santiniketan Sahityapath

- XAI-RNN-SGRU মডেল ৯৯.৯৯% নির্ভুলতা অর্জন করেছে, জালিয়াতি সনাক্তকরণ ও ডেটা এনক্রিপশনে বিপ্লব ঘটিয়েছে (Ghosh, 2025)
- ব্লকচেইন-ভিত্তিক বিশ্ববিদ্যালয় পরীক্ষা ব্যবস্থা স্কোর ম্যানিপুলেশন ও সার্টিফিকেট জালিয়াতি রোধ করতে সক্ষম, ট্রেসেবিলিটি ও স্বচ্ছতা নিশ্চিত করেছে (Samanta & Sarkar, 2021)।
- সাপ্লাই চেইনে ব্লকচেইন প্রয়োগ ডেটা টেম্পারিং কমিয়েছে, চালের সাপ্লাই চেইন কেস স্টাডিতে ডেটা অখণ্ডতা ও গুণমান নিয়ন্ত্রণ নিশ্চিত করেছে (Samanta, 2021)।
- সাইবিল আক্রমণ প্রতিরোধে গেম-ভিত্তিক মডেল প্রস্তাব করা হয়েছে, যা বিকেন্দ্রীভূত নেটওয়ার্কে নিরাপদ লেনদেনের সম্ভাবনা উন্মোচন করেছে (Samanta & Chaki, 2023)।

৪.২. গবেষণার ফাঁক (Gaps)

ইউএভি ইকোসিস্টেমে ফেডারেটেড লার্নিং-এর বাস্তব-বিশ্বের প্রয়োগ ও নিয়ন্ত্রণ কাঠামোর অভাব (Farsi et al., 2025)। বিগ ডেটা সিস্টেমে অ্যাক্সেস নিয়ন্ত্রণ ও শেষাধিকারপ্রাপ্ত ব্যবহারকারীদের জন্য গাণিতিক মডেলের সীমাবদ্ধতা (Poltavtseva et al., 2024)। ইথেরিয়াম বীকন চেইনের ভিজ্যুয়াল অ্যানালিটিক টুলের কার্যকারিতা শুধুমাত্র ঐতিহাসিক ডেটা বিশ্লেষণে সীমাবদ্ধ (Chen et al., 2024)। ক্যাওটিক সিস্টেম-ভিত্তিক এনক্রিপশন মডেলের স্কেলেবিলিটি ও বিভিন্ন শিল্পে প্রয়োগের অভিজ্ঞতা (Hua et al., 2023)। XAI-RNN-SGRU মডেলের উচ্চ নির্ভুলতা সত্ত্বেও জটিলতা ও কম্পিউটেশনাল খরচের সমস্যা (Ghosh, 2025)। সাইবিল আক্রমণ প্রতিরোধে প্রস্তাবিত গেম-ভিত্তিক মডেলের বাস্তবায়ন ও কার্যকারিতা মূল্যায়নের অভাব (Samanta & Chaki, 2023)। ব্লকচেইন-ভিত্তিক বিশ্ববিদ্যালয় পরীক্ষা ব্যবস্থায় স্কেলেবিলিটি এবং বিভিন্ন শিক্ষা প্রতিষ্ঠানে প্রয়োগের চ্যালেঞ্জ (Samanta & Sarkar, 2021)। ইআইএস-এর জন্য বিগ ডেটা-ভিত্তিক ঝুঁকি ভবিষ্যদ্বাণী মডেলের শিল্প-নির্দিষ্ট অভিযোজন ও ডিপ লার্নিং প্রযুক্তির সম্পূর্ণ একীকরণের অভাব (Li & Zhang, 2025)।

৪.৩ গবেষণার অনুপ্রেরণা এবং প্রস্তাবিত নকশার ভিত্তি (Research Motivation and Design Rationale)

প্রাসঙ্গিক গবেষণাসমূহের বিশ্লেষণে দেখা যায় যে বিভিন্ন গবেষক ডেটা নিরাপত্তা, গোপনীয়তা, ব্লকচেইন-ভিত্তিক লেনদেন, ফেডারেটেড লার্নিং, বিগ ডেটা নিরাপত্তা এবং সাইবার আক্রমণ প্রতিরোধের জন্য বিভিন্ন কার্যকর সমাধান প্রস্তাব করেছেন। তবে বিদ্যমান গবেষণাগুলির অধিকাংশই নির্দিষ্ট অ্যাপ্লিকেশন ক্ষেত্র, যেমন আর্থিক লেনদেন, বিশ্ববিদ্যালয় পরীক্ষা ব্যবস্থা, মহাকাশ তথ্য নেটওয়ার্ক অথবা শিল্পভিত্তিক তথ্য ব্যবস্থার মধ্যে সীমাবদ্ধ।

সাহিত্য পর্যালোচনা থেকে প্রাপ্ত গবেষণার ঘাটতি বিশ্লেষণ করে দেখা যায় যে সামাজিক তথ্যের জন্য একটি সমন্বিত, বিকেন্দ্রীভূত এবং পরিবর্তন-প্রতিরোধী নিরাপত্তা কাঠামো এখনো পর্যাপ্তভাবে উপস্থাপিত হয়নি। বিশেষত ব্যবহারকারী প্রমাণীকরণ, তথ্য যাচাইকরণ, ক্রিপ্টোগ্রাফিক অখণ্ডতা যাচাই, ব্লকচেইন-ভিত্তিক ট্রেসেবিলিটি এবং পরিবর্তন শনাক্তকরণকে একই নিরাপত্তা কাঠামোর মধ্যে একত্রিত করার বিষয়ে বিদ্যমান গবেষণায় স্পষ্ট সমাধান পাওয়া যায়নি। এই সীমাবদ্ধতাগুলোর ভিত্তিতেই বর্তমান গবেষণায় একটি Blockchain-based Social Data Security Framework প্রস্তাব করা হয়েছে। প্রস্তাবিত কাঠামোতে Authentication Layer, Validation Layer, SHA-256 Hash Generation, Blockchain Ledger, Consensus Verification এবং Audit Layer সমন্বিতভাবে কাজ করে, যাতে সামাজিক তথ্যের গোপনীয়তা, অখণ্ডতা, ট্রেসেবিলিটি এবং পরিবর্তন-প্রতিরোধ ক্ষমতা নিশ্চিত করা যায়। অতএব, বর্তমান গবেষণার নকশা পূর্ববর্তী গবেষণাগুলির বিকল্প নয়; বরং সেসব গবেষণায় চিহ্নিত সীমাবদ্ধতাগুলির সমন্বিত সমাধান প্রদানের উদ্দেশ্যে পরিকল্পিত একটি সম্প্রসারিত নিরাপত্তা কাঠামো।

৫. পদ্ধতি (Methodology)

বর্তমান গবেষণার পদ্ধতিগত কাঠামোটি প্রাসঙ্গিক গবেষণাসমূহে চিহ্নিত সীমাবদ্ধতার উপর ভিত্তি করে পরিকল্পিত হয়েছে। সাহিত্য পর্যালোচনায় প্রাপ্ত গবেষণার ঘাটতিগুলির বিশ্লেষণ থেকে যে নকশাগত প্রয়োজনীয়তাগুলি নির্ধারণ করা হয়েছে, সেগুলোর সমন্বয়েই প্রস্তাবিত Blockchain-based Social Data Security Framework নির্মিত হয়েছে। অতএব, Methodology অংশে বর্ণিত প্রতিটি

© Santiniketan Sahityapath

উপাদান সরাসরি Literature Reviewএ চিহ্নিত সমস্যার সমাধানের উদ্দেশ্যে অন্তর্ভুক্ত করা হয়েছে। এই গবেষণাপত্রে প্রস্তাবিত সমাধানটি দুটি ধাপে উপস্থাপিত হয়েছে। প্রথম ধাপে, বিশ্ববিদ্যালয়ের ভর্তি ব্যবস্থায় ব্লকচেইন প্রযুক্তির সংযোজনের পরামর্শ দেওয়া হয়েছে। ব্লকচেইন প্রয়োগের উপযোগিতা হলো তথ্য অপরিবর্তনীয় এবং হস্তক্ষেপ-প্রতিরোধী হবে যা তথ্যের বিশ্বস্ততা বাড়াবে। আবেদনকারী এবং বিশ্ববিদ্যালয়ের মধ্যে স্মার্ট কন্ট্রাক্ট সুবিধার সংযোজনের মাধ্যমে, ব্যবস্থাটি প্রথমত কাগজপত্র-মুক্ত হবে এবং নিরাপদ তথ্য সংরক্ষণের মাধ্যমে তথ্যের গোপনীয়তা বজায় রাখা যাবে। এই সমাধানে, আমরা হাইপারলেজার ব্যবহার করে একটি প্রাইভেট ব্লকচেইন-ভিত্তিক ভর্তি ব্যবস্থার জন্য একটি স্মার্ট কন্ট্রাক্ট অ্যাপ্লিকেশন তৈরি করেছি। এই গবেষণার মূল উদ্দেশ্য হলো সামাজিক তথ্য (Social Data) এর নিরাপত্তা নিশ্চিত করার জন্য একটি ব্লকচেইন-ভিত্তিক নিরাপদ কাঠামো (Blockchain-based Secure Social Data Security Framework) প্রস্তাব করা। বর্তমান অধিকাংশ সামাজিক তথ্য কেন্দ্রীভূত (Centralized) সার্ভারে সংরক্ষিত হয়, ফলে ডেটা পরিবর্তন, অননুমোদিত প্রবেশ, পরিচয় জালিয়াতি এবং ডেটা লঙ্ঘনের ঝুঁকি বিদ্যমান থাকে। এই সমস্যার সমাধানে গবেষণায় একটি Permissioned Blockchain ভিত্তিক নিরাপদ ডেটা ব্যবস্থাপনা কাঠামো প্রস্তাব করা হয়েছে। এখানে প্রতিটি সামাজিক তথ্য একটি স্বতন্ত্র ব্লকে সংরক্ষিত হয় এবং SHA-256 ক্রিপ্টোগ্রাফিক হ্যাশ দ্বারা পূর্ববর্তী ব্লকের সঙ্গে সংযুক্ত থাকে। ফলে কোনো ব্যবহারকারী পূর্ববর্তী তথ্য পরিবর্তনের চেষ্টা করলে সমগ্র ব্লকচেইনের অখণ্ডতা নষ্ট হয়ে যায় এবং পরিবর্তন সহজেই শনাক্ত করা সম্ভব হয়।

প্রস্তাবিত কাঠামোতে ব্যবহারকারী পরিচয় যাচাই (Authentication), ডেটা এনক্রিপশন, ডিজিটাল স্বাক্ষর, টাইমস্ট্যাম্প, ডিস্ট্রিবিউটেড লেজার এবং কনসেনসাস মেকানিজম একত্রে কাজ করে। ফলে সামাজিক তথ্যের গোপনীয়তা (Confidentiality), অখণ্ডতা (Integrity), প্রাপ্যতা (Availability) এবং ট্রেসেবিলিটি (Traceability) নিশ্চিত হয়। এই গবেষণায় Hyperledger Fabricকে কোনো নির্দিষ্ট বিশ্ববিদ্যালয়ের ভর্তি ব্যবস্থার জন্য নয়; বরং একটি Permissioned Blockchain Framework এর উদাহরণ হিসেবে আলোচনা করা হয়েছে। পরবর্তীতে Python-ভিত্তিক একটি Proof-of-Concept Prototype তৈরি করে প্রস্তাবিত নিরাপত্তা কাঠামোর কার্যকারিতা প্রদর্শন করা হয়েছে।

৫.১. ব্লকচেইন প্রযুক্তির মূল উপাদান

ব্লকচেইন প্রযুক্তি ডেটা শেয়ারিংয়ের নিরাপত্তা ক্ষেত্রে একটি চাহিদাসম্পন্ন প্রযুক্তি। ব্লকচেইনের অপরিবর্তনীয় বৈশিষ্ট্য লেনদেনের ডেটাকে স্বচ্ছ এবং বিশ্বস্ত করে তোলে। ব্লকচেইন হলো একটি ক্রমাগত বর্ধনশীল ডেটাবেস চেইন যা স্থায়ী রেকর্ড বা "ব্লক" নিয়ে গঠিত, যেগুলি ক্রিপ্টোগ্রাফি-ভিত্তিক হ্যাশ ফাংশন ব্যবহার করে সংযুক্ত এবং সুরক্ষিত থাকে (চিত্র ২)। ব্লকচেইনটি নির্দিষ্ট অ্যাপ্লিকেশন ক্ষেত্রের উপর নির্ভর করে পাবলিক, প্রাইভেট, বা কনসোর্টিয়াম নেটওয়ার্ক হিসেবে ডিজাইন করা হয়। প্রাইভেট ব্লকচেইনের ক্ষেত্রে ডেটাবেস অ্যাক্সেস করতে এবং কোনো লেনদেন করতে অনুমতি প্রয়োজন। পাবলিক ব্লকচেইনের ক্ষেত্রে, নেটওয়ার্কগুলি যে কাউকে নেটওয়ার্কে অংশগ্রহণের অনুমতি দেয়। ডেটাবেসটি অ্যাক্সেসের জন্য উন্মুক্ত, এবং নেটওয়ার্কে যোগদানের জন্য কোনো অনুমতির প্রয়োজন হয় না। কনসোর্টিয়াম ব্লকচেইনের ক্ষেত্রে, কিছু সাধারণ উদ্দেশ্য এবং পারস্পরিক চুক্তি থাকতে হবে। ব্লকচেইনের ব্লক কাঠামো হলো ব্লকচেইন লেজারের মৌলিক একক। প্রতিটি ব্লক ডেটার একটি সংগ্রহ (সাধারণত লেনদেন) এবং মেটাডেটা ধারণ করে যা এটিকে পূর্ববর্তী ব্লকের সঙ্গে নিরাপদে সংযুক্ত করে। এখানে একটি সাধারণ ব্লক কাঠামোর বিবরণ দেওয়া হলো (চিত্র ২):

© Santiniketan Sahityapath

চিত্র ২: ব্লকচেইনের ব্লক কাঠামো

ক. ব্লক হেডার: হেডারে ব্লক সম্পর্কিত মেটাডেটা থাকে এবং ব্লকগুলিকে একসঙ্গে সংযুক্ত করার জন্য এটি অত্যন্ত গুরুত্বপূর্ণ। ব্লক হেডারে নিম্নলিখিত মূল উপাদানসমূহ থাকে:

- ব্লক ভার্সন: ব্লকচেইন প্রোটোকলের কোন্ সংস্করণ ব্যবহৃত হয়েছে তা নির্দেশ করে।
- মার্কল রুট: ব্লকের সকল লেনদেনের প্রতিনিধিত্বকারী একটি একক হ্যাশ। এটি মার্কল ট্রি কাঠামো থেকে উদ্ভূত হয়।
- টাইমস্ট্যাম্প: ব্লকটি কখন তৈরি হয়েছিল তা নির্দেশ করে (ইউনিক্স টাইমস্ট্যাম্প)।
- ডিফিকাল্টি টার্গেট: মাইনিং প্রক্রিয়ার সময়ে অসুবিধার মাত্রা (প্রুফ-অফ-ওয়ার্ক সিস্টেমে ব্যবহৃত)।
- নন্স: মাইনিংয়ে ব্যবহৃত একটি সংখ্যা যা অসুবিধার প্রয়োজনীয়তা পূরণ করে বৈধ ব্লক হ্যাশ খুঁজে বের করতে ব্যবহৃত হয়।
- পূর্ববর্তী ব্লক হ্যাশ: পূর্ববর্তী ব্লকের হেডারের একটি ক্রিপ্টোগ্রাফিক হ্যাশ, যা চেইনের অখণ্ডতা ও অপরিবর্তনীয়তা নিশ্চিত করে।
- বর্তমান হ্যাশ মান: বর্তমান ব্লকের হেডারের ক্রিপ্টোগ্রাফিক হ্যাশ, যা ব্লকের সকল ডেটার অখণ্ডতা প্রতিনিধিত্ব করে এবং পরবর্তী ব্লকের জন্য রেফারেন্স হিসেবে ব্যবহৃত হয়।

খ. ব্লক বডি: ব্লক বডিতে নিম্নলিখিত মূল উপাদানসমূহ থাকে:

- লেনদেন কাউন্টার: ব্লকে কতগুলি লেনদেন রয়েছে তা নির্দেশ করে।
- লেনদেন: ব্লকে অন্তর্ভুক্ত সকল লেনদেনের তালিকা। প্রতিটি লেনদেনে প্রেরক, গ্রহীতা, পরিমাণ, ডিজিটাল স্বাক্ষর এবং অন্যান্য মেটাডেটা থাকতে পারে।

© Santiniketan Sahityapath

ব্লকচেইনের ব্লকগুলির শৃঙ্খল (চিত্র ২) মেটা-টেকনোলজির মাধ্যমে তথ্য ধারণ করে। এই প্রযুক্তি প্রতিটি ডিজিটাল লেনদেনে টাইমস্ট্যাম্প প্রক্রিয়ার মাধ্যমে ডেটা সংরক্ষণ করে যা ডেটাকে নিরাপদ রাখে এবং এর সঙ্গো ছেদখণ্ড করা কঠিন করে। এটি একটি বিতরিত লেজার যা সম্পূর্ণরূপে সকল ব্যবহারকারীর জন্য উন্মুক্ত। কেন্দ্রীয় সত্তার পরিবর্তে, ব্লকচেইন একটি পিয়ার-টু-পিয়ার বিতরিত সিস্টেম হিসেবে ব্যবহৃত হয়। যখন একজন নতুন ব্যবহারকারী এই নেটওয়ার্কে যোগ দেন, তিনি ব্লকচেইনের একটি সম্পূর্ণ কপি পান, যাতে শুধুমাত্র পড়ার অধিকার থাকে। ব্লকচেইনের প্রতিটি ব্লকে কিছু ডেটা, ব্লকের অনন্য হ্যাশ মান এবং পূর্ববর্তী ব্লকের হ্যাশ মান থাকে। প্রথম ব্লকে পূর্ববর্তী ব্লকের হ্যাশ মান থাকে না, যাকে "জেনেসিস" ব্লক বলা হয়। যখনই একটি ব্লক তৈরি হয়, তখনি এর হ্যাশ মান গণনা করা হয়। ব্লকের ডেটার সঙ্গো ছেদখণ্ড করলে এর হ্যাশ মান পরিবর্তিত হয় এবং বাকি ব্লকের শৃঙ্খলের সঙ্গো মেলে না। এই কৌশলটি ব্লকচেইনকে নিরাপদ করে। হ্যাশগুলি অত্যন্ত উপযোগী এবং ব্লকের আঙুলের ছাপ হিসেবে কাজ করে। যখন কেউ একটি নতুন ব্লক তৈরি করে, তখন সেই ব্লকটি নেটওয়ার্কের সকলের কাছে পাঠানো হয়। প্রতিটি নোড তখন ব্লকটি যাচাই করে নিশ্চিত করে যে এর সঙ্গো কোনো ছেদখণ্ড করা হয়নি। যদি সবকিছু সঠিক হয়, তবে প্রতিটি নোডের যাচাইয়ের পর ব্লকটি ব্লকচেইনে যুক্ত হয়। এই নেটওয়ার্কের সকল নোড কোন্ ব্লকগুলি বৈধ এবং কোন্‌টি অবৈধ তা নিয়ে ঐকমত্য তৈরি করে। যে-কোনো ছেদখণ্ডকৃত ব্লক নেটওয়ার্কের অন্যান্য নোড দ্বারা প্রত্যাখ্যাত হয়।

বর্তমান গবেষণার প্রধান নতুনত্ব (Novel Contribution) কেবল ব্লকচেইনের মৌলিক উপাদান বর্ণনায় সীমাবদ্ধ নয়; বরং সামাজিক তথ্যের নিরাপত্তা নিশ্চিত করার জন্য একটি সমন্বিত নিরাপত্তা স্থাপত্য (Blockchain-based Social Data Security Architecture) প্রস্তাব করা হয়েছে। এই স্থাপত্যে প্রতিটি তথ্য প্রথমে ব্যবহারকারী প্রমাণীকরণ (Authentication) স্তর অতিক্রম করে। এরপর তথ্যের বৈধতা যাচাই (Validation) সম্পন্ন হয় এবং SHA-256 অ্যালগরিদমের মাধ্যমে একটি অনন্য হ্যাশ মান তৈরি করা হয়। হ্যাশকৃত তথ্য ব্লকচেইন লেজারে সংরক্ষিত হয়, যেখানে পূর্ববর্তী ব্লকের হ্যাশের সঙ্গো ক্রিপ্টোগ্রাফিকভাবে সংযুক্ত থাকে। কনসেনসাস যাচাইকরণের পর তথ্যটি বিতরণকৃত লেজারে সংরক্ষিত হয় এবং একটি স্বয়ংক্রিয় অডিট স্তর ভবিষ্যতের যে-কোনো পরিবর্তন শনাক্ত করতে সক্ষম হয়।

ফলে প্রস্তাবিত স্থাপত্য সামাজিক তথ্যের গোপনীয়তা, অখণ্ডতা, ট্রেসেবিলিটি এবং পরিবর্তন-প্রতিরোধ ক্ষমতা নিশ্চিত করে, যা প্রচলিত কেন্দ্রীভূত তথ্য ব্যবস্থার তুলনায় অধিক নিরাপদ ও নির্ভরযোগ্য।

৫.২. ব্লকচেইন প্রযুক্তির নিরাপত্তা বৈশিষ্ট্য

ব্লকচেইনের নিরাপত্তা এবং গোপনীয়তা বজায় রাখতে প্রুফ অফ ওয়ার্ক (PoW), প্রুফ অফ স্টেক (PoS), ডেলিগেটেড প্রুফ অফ স্টেক (DPoS), প্রুফ অফ ক্যাপাসিটি (PoC), প্রুফ অফ অথরিটি (PoA), প্রুফ অফ ইল্যাপসড টাইম (PoET), এবং প্রুফ অফ ইমপর্ট্যান্স (PoI) এর মতো কনসেনসাস অ্যালগরিদম ব্যবহার করা হয়। হাইপারলেজার ফ্যাব্রিক, বিটকয়েন, ইথেরিয়াম, ইওএসআইও, কোড্রা হলো ব্লকচেইন নেটওয়ার্ক তৈরির জন্য ব্যবহৃত গুরুত্বপূর্ণ জনপ্রিয় ফ্রেমওয়ার্ক।

- ব্লকচেইন ফ্রেমওয়ার্কের ক্রিপ্টোগ্রাফিক ভিত্তিক অ্যাপ্লিকেশনে।
- ব্লকচেইন ফ্রেমওয়ার্ক নেটওয়ার্কের সমস্ত লেনদেনের লেজারকে বিতরণকৃত পরিবেশে সমর্থন করে।
- ব্লকচেইন পাবলিক, প্রাইভেট এবং কনসোর্টিয়াম ব্লকচেইন মোডে বাস্তবায়ন করা যায়।
- ব্লকচেইন প্রযুক্তি অপরিবর্তনীয় এবং হস্তক্ষেপ-প্রতিরোধী, যা তথ্যের দৃঢ়তা এবং বিশ্বস্ততা বাড়ায়।

© Santiniketan Sahityapath

চিত্র ৩: ব্লকচেইন প্রযুক্তির নিরাপত্তার বৈশিষ্ট্য

- ব্লকচেইন কনসেনসাস-চালিত অ্যালগরিদমে কাজ করে, যেমন প্রুফ অফ ওয়ার্ক (PoW), প্রুফ অফ স্টেক (PoS) ইত্যাদি।
- ব্লকচেইন ফ্রেমওয়ার্ক স্মার্ট কন্ট্রাক্ট সমর্থন করে, যা তৃতীয় পক্ষের সম্পৃক্ততা ছাড়াই দুই পক্ষের মধ্যে কাগজপত্র-বিহীন লেনদেন এবং চুক্তির সুবিধা দেয়।

অতএব, তথ্যের জন্য সর্বদা একটি হুমকি থাকে, এবং এই হুমকিগুলি বাহ্যিক এবং অভ্যন্তরীণ উভয়ই। গবেষকরা সর্বদা এই হুমকিগুলি প্রশমনের জন্য সমাধানের তালিকা প্রদান করে। এই নির্দিষ্ট নিবন্ধে, আমরা ব্লকচেইন প্রবর্তনের মাধ্যমে এই হুমকির সমস্যাগুলি সমাধান করার চেষ্টা করেছি।

প্রস্তাবিত নিরাপত্তা কাঠামোর কার্যপ্রবাহ নিম্নরূপ:

(১) ব্যবহারকারী সামাজিক তথ্য জমা দেয়।

(২) তথ্য যাচাইকরণ ও ডিজিটাল স্বাক্ষর সম্পন্ন হয়।

(৩) SHA-256 হ্যাশ তৈরি করা হয়।

(৪) নতুন ব্লক তৈরি করা হয়।

(৫) পূর্ববর্তী ব্লকের হ্যাশ সংযুক্ত করা হয়।

(৬) কনসেনসাস যাচাইকরণ সম্পন্ন হয়।

(৭) ব্লকটি ডিস্ট্রিবিউটেড লেজারে সংরক্ষিত হয়।

(৮) ভবিষ্যতে যে-কোনো পরিবর্তন ব্লকচেইন যাচাইয়ের মাধ্যমে শনাক্ত করা যায়।

© Santiniketan Sahityapath

সারণি ১: প্রচলিত ব্লকচেইন কাঠামো এবং প্রস্তাবিত সামাজিক তথ্য নিরাপত্তা কাঠামোর তুলনা

বৈশিষ্ট্য	প্রচলিত ব্লকচেইন	প্রস্তাবিত কাঠামো
উদ্দেশ্য	সাধারণ লেনদেন	সামাজিক তথ্য সুরক্ষা
তথ্য যাচাইকরণ	মৌলিক	বহুস্তরীয়
হ্যাশ	SHA-256	SHA-256 + Validation Layer
সংরক্ষণ	Blockchain	Blockchain + Audit Layer
ট্রেসেবিলিটি	সাধারণ	উন্নত
পরিবর্তন শনাক্তকরণ	সীমিত	তাৎক্ষণিক

উল্লেখ্য যে, Hyperledger Fabric এই গবেষণায় একটি সম্ভাব্য Permissioned Blockchain Frameworkএর উদাহরণ হিসেবে আলোচনা করা হয়েছে। তবে বর্তমান গবেষণার পরীক্ষামূলক বাস্তবায়ন Hyperledger Fabric Networkএর উপর পরিচালিত হয়নি। বরং প্রস্তাবিত নিরাপত্তা কাঠামোর কার্যকারিতা প্রদর্শনের জন্য Python-ভিত্তিক একটি Blockchain Prototype তৈরি করা হয়েছে। ভবিষ্যৎ গবেষণায় Hyperledger Fabric, Chaincode এবং Smart Contract ব্যবহার করে পূর্ণাঙ্গ Permissioned Blockchain বাস্তবায়নের পরিকল্পনা রয়েছে।

এই গবেষণার মূল প্রযুক্তিগত অবদান একটি Python-ভিত্তিক ব্লকচেইন প্রোটোটাইপ নির্মাণ ও তার মাধ্যমে প্রস্তাবিত সামাজিক তথ্য নিরাপত্তা কাঠামোর কার্যকারিতা যাচাই করা। Hyperledger Fabric এবং Ethereum Framework এই গবেষণায় পূর্ণাঙ্গ বাস্তবায়নের প্ল্যাটফর্ম হিসেবে ব্যবহৃত হয়নি; বরং Permissioned এবং Public Blockchain প্রযুক্তির প্রতিনিধিত্বকারী উদাহরণ হিসেবে সাহিত্য পর্যালোচনা ও তাত্ত্বিক আলোচনায় উল্লেখ করা হয়েছে। ফলে গবেষণার পরীক্ষামূলক অংশ সম্পূর্ণরূপে Python Prototypeএর উপর ভিত্তি করে পরিচালিত হয়েছে।

৬. প্রস্তাবিত নিরাপত্তা কাঠামোর বাস্তবায়ন এবং ফলাফল

প্রস্তাবিত সামাজিক তথ্য নিরাপত্তা কাঠামোর কার্যকারিতা যাচাই করার জন্য একটি Python-ভিত্তিক Blockchain Prototype তৈরি করা হয়েছে। এই Prototype গবেষণার Concept Validation হিসেবে ব্যবহৃত হয়েছে। এখানে প্রতিটি সামাজিক তথ্য SHA-256 Hash দ্বারা সুরক্ষিত ব্লকে সংরক্ষিত হয় এবং পূর্ববর্তী ব্লকের Hashএর সঙ্গে সংযুক্ত থাকে। Prototypeএর উদ্দেশ্য কোনো পূর্ণাঙ্গ বাণিজ্যিক সফটওয়্যার তৈরি করা নয়; বরং প্রস্তাবিত নিরাপত্তা মডেলের কার্যকারিতা পরীক্ষামূলকভাবে প্রদর্শন করা। প্রস্তাবিত সামাজিক তথ্য নিরাপত্তা কাঠামোর কার্যকারিতা যাচাই করার জন্য Python 3.11.10 পরিবেশে একটি Proof-of-Concept Blockchain Prototype তৈরি করা হয়েছে। কোড উন্নয়নের জন্য Spyder IDE এবং Sublime Text ব্যবহার করা হয়েছে। গবেষণার উদ্দেশ্য ছিল কোনো বাণিজ্যিক ব্লকচেইন প্ল্যাটফর্মের বিকল্প তৈরি করা নয়; বরং সামাজিক তথ্য সংরক্ষণে ব্লকচেইনের মৌলিক নিরাপত্তা বৈশিষ্ট্য পরীক্ষামূলকভাবে প্রদর্শন করা।

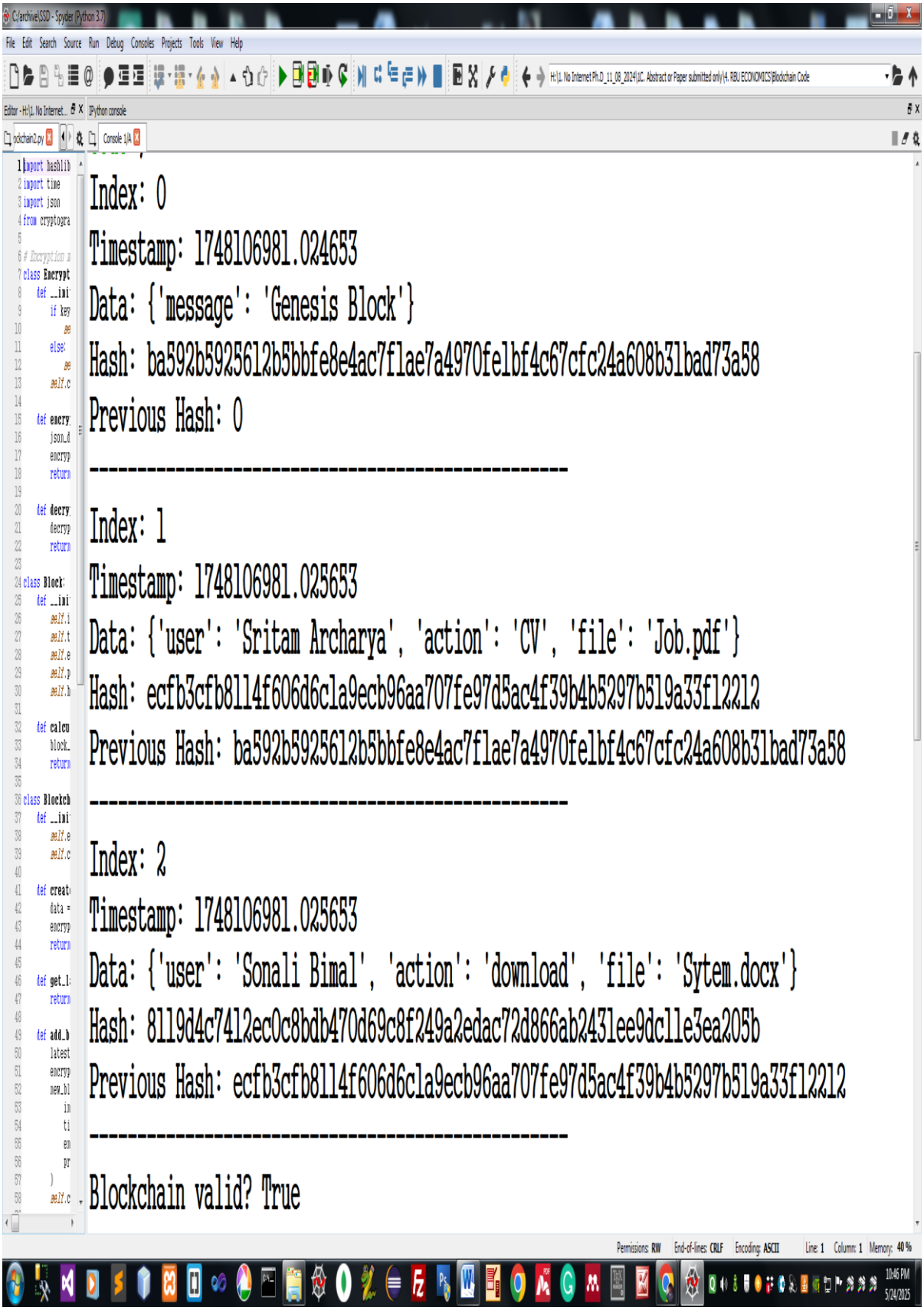
Prototypeএ প্রতিটি ব্লকে Index, Timestamp, Transaction Data, Previous Block Hash এবং Current Block Hash সংরক্ষণ করা হয়েছে। SHA-256 ক্রিপ্টোগ্রাফিক হ্যাশ অ্যালগরিদম ব্যবহার করে প্রতিটি ব্লকের হ্যাশ গণনা করা হয়েছে এবং নতুন ব্লককে পূর্ববর্তী ব্লকের হ্যাশের সঙ্গে সংযুক্ত করা হয়েছে। এর ফলে কোনো ব্লকের তথ্য পরিবর্তিত হলে পরবর্তী সমস্ত ব্লকের হ্যাশ অকার্যকর হয়ে যায় এবং ব্লকচেইনের অখণ্ডতা (Integrity) যাচাই করা সম্ভব হয়।

Prototypeএর কার্যকারিতা মূল্যায়নের জন্য একাধিক নমুনা সামাজিক তথ্য (Sample Social Data Transactions) ব্লকচেইনে সংযোজন করা হয়েছে। প্রতিটি লেনদেনের পর ব্লকচেইনের বৈধতা (Blockchain Validity) যাচাই করা হয়েছে এবং পরিবর্তন শনাক্তকরণ (Tamper Detection) পরীক্ষাও সম্পন্ন করা হয়েছে। পরীক্ষার ফলাফল থেকে দেখা যায় যে তথ্য পরিবর্তনের যেকোনো প্রচেষ্টা সঙ্গে সঙ্গে হ্যাশের অসামঞ্জস্য সৃষ্টি করে, ফলে অনুমোদিত পরিবর্তন সহজেই সনাক্ত করা যায়।

© Santiniketan Sahityapath

চিত্র ৪: ব্লকচেইন প্রযুক্তির নিরাপত্তার বৈশিষ্ট্য

© Santiniketan Sahityapath



চিত্র ৫: ব্লকচেইন প্রযুক্তির নিরাপত্তার বৈশিষ্ট্য

প্রস্তাবিত প্রোটোটাইপের পরীক্ষায় প্রতিটি নতুন সামাজিক তথ্য একটি পৃথক ব্লকে সংরক্ষিত হয়েছে এবং SHA-256 অ্যালগরিদমের মাধ্যমে তার হ্যাশ সফলভাবে তৈরি হয়েছে। পরীক্ষায় দেখা যায় যে-কোনো ব্লকের তথ্য পরিবর্তন করা হলে সংশ্লিষ্ট ব্লকের হ্যাশ পরিবর্তিত হয় এবং পরবর্তী ব্লকগুলোর সঙ্গে সংযোগ বিচ্ছিন্ন হয়ে যায়। ফলে ব্লকচেইন যাচাইকরণ প্রক্রিয়া চেইনটিকে

© Santiniketan Sahityapath

অবৈধ (Invalid) হিসেবে সনাক্ত করে। এই ফলাফল নির্দেশ করে যে প্রস্তাবিত কাঠামো সামাজিক তথ্যের অখণ্ডতা (Integrity), ট্রেসেবিলিটি (Traceability) এবং পরিবর্তন-প্রতিরোধ ক্ষমতা (Tamper Resistance) নিশ্চিত করতে সক্ষম।

৭. আলোচনা (Discussion)

বর্তমান গবেষণায় প্রস্তাবিত Blockchain-based Social Data Security Frameworkএর ফলাফলকে প্রাসঙ্গিক সাম্প্রতিক গবেষণার সঙ্গে তুলনামূলকভাবে বিশ্লেষণ করা হয়েছে। সাহিত্য পর্যালোচনায় অন্তর্ভুক্ত গবেষণাগুলো (২০২৪-২০২৫) বিভিন্ন নির্দিষ্ট ক্ষেত্রে ডেটা নিরাপত্তা উন্নয়নের জন্য পৃথক প্রযুক্তি ও কাঠামো প্রস্তাব করেছে। যেমন Zhu এবং Wang (2025) বিশ্বস্ত তথ্য আদান-প্রদানের জন্য Trusted Platform Module (TPM) ও Trusted Execution Environment (TEE)এর সমন্বিত কাঠামো উপস্থাপন করেছেন। Li এবং Zhang (2025) বিগ ডেটা-ভিত্তিক ঝুঁকি বিশ্লেষণে গুরুত্ব দিয়েছেন। Chen এবং সহকর্মীরা (2024) Ethereum Consensus Layerএ নিরাপত্তা হুমকি সনাক্তকরণের জন্য একটি Visual Analytics Framework প্রস্তাব করেছেন। Ghosh (2025) আর্থিক সাইবার নিরাপত্তার জন্য Explainable AI-ভিত্তিক মডেল উপস্থাপন করেছেন।

বর্তমান গবেষণার উদ্দেশ্য উল্লিখিত গবেষণাগুলির বিকল্প তৈরি করা নয়; বরং সামাজিক তথ্য নিরাপত্তার জন্য একটি সমন্বিত ব্লকচেইন-ভিত্তিক কাঠামো প্রস্তাব করা। বিদ্যমান গবেষণার অধিকাংশই নির্দিষ্ট অ্যাপ্লিকেশনভিত্তিক নিরাপত্তা সমাধান প্রদান করলেও, বর্তমান গবেষণায় Authentication, Data Validation, SHA-256 Hash Verification, Blockchain Ledger এবং Audit Mechanismকে একই কাঠামোর মধ্যে একত্রিত করা হয়েছে। Python-ভিত্তিক Proof-of-Concept Prototypeএর মাধ্যমে প্রস্তাবিত কাঠামোর কার্যকারিতা পরীক্ষামূলকভাবে প্রদর্শন করা হয়েছে। পরীক্ষায় দেখা যায় যে তথ্য পরিবর্তনের ক্ষেত্রে হ্যাশ যাচাইকরণ প্রক্রিয়া দ্রুত অসামঞ্জস্য শনাক্ত করতে সক্ষম হয়, যা ব্লকচেইনের অখণ্ডতা রক্ষায় কার্যকর। যদিও এই গবেষণায় Enterprise Blockchain Platform (যেমন Hyperledger Fabric বা Ethereum)এ বাস্তবায়ন করা হয়নি, তবুও প্রস্তাবিত কাঠামো ভবিষ্যতে Permissioned Blockchain Platformএ বাস্তবায়নের জন্য একটি ভিত্তিমূলক নকশা (Foundational Architecture) হিসেবে বিবেচিত হতে পারে। অতএব, বর্তমান গবেষণার প্রধান অবদান হলো একটি সমন্বিত সামাজিক তথ্য নিরাপত্তা কাঠামো উপস্থাপন করা, যা সাহিত্য পর্যালোচনায় চিহ্নিত বিভিন্ন সীমাবদ্ধতাকে একত্রে সমাধানের প্রচেষ্টা করেছে এবং ভবিষ্যৎ বাস্তবায়নের জন্য একটি গবেষণা-ভিত্তিক ভিত্তি প্রদান করেছে।

৮. সীমাবদ্ধতা

যদিও বর্তমান গবেষণায় সামাজিক তথ্যের নিরাপত্তা নিশ্চিত করার জন্য একটি ব্লকচেইন-ভিত্তিক নিরাপত্তা কাঠামো প্রস্তাব করা হয়েছে এবং Python-ভিত্তিক একটি Proof-of-Concept Prototypeএর মাধ্যমে এর কার্যকারিতা প্রদর্শন করা হয়েছে, তবুও গবেষণাটির কিছু সীমাবদ্ধতা রয়েছে।

প্রথমত, গবেষণায় উপস্থাপিত প্রোটোটাইপটি পরীক্ষামূলক (Prototype) পর্যায়ে সীমাবদ্ধ এবং এটি বাস্তব সামাজিক তথ্যভান্ডার বা বৃহৎ পরিসরের (Large-scale) পরিবেশে পরীক্ষা করা হয়নি। ফলে উচ্চমাত্রার ব্যবহারকারী, বিপুল পরিমাণ লেনদেন এবং বাস্তব নেটওয়ার্ক পরিবেশে এর কর্মক্ষমতা (Performance), স্কেলেবিলিটি (Scalability) এবং স্থায়িত্ব (Stability) এই গবেষণায় মূল্যায়ন করা সম্ভব হয়নি।

দ্বিতীয়ত, বর্তমান গবেষণায় SHA-256 ভিত্তিক হ্যাশ যাচাইকরণ ব্যবহার করে তথ্যের অখণ্ডতা (Integrity) এবং পরিবর্তন-প্রতিরোধ ক্ষমতা (Tamper Resistance) প্রদর্শন করা হয়েছে। তবে উন্নত Consensus Mechanism, Smart Contract, Byzantine Fault Tolerance, অথবা Enterprise Blockchain Platform (যেমন Hyperledger Fabric বা Ethereum)এ পূর্ণাঙ্গ বাস্তবায়ন এই গবেষণার আওতাভুক্ত ছিল না।

তৃতীয়ত, ব্লকচেইন প্রযুক্তির নিজস্ব কিছু সীমাবদ্ধতা রয়েছে। বিশেষ করে Proof-of-Work (PoW) ভিত্তিক নেটওয়ার্কে অধিক বিদ্যুৎ খরচ, উচ্চ কম্পিউটেশনাল ব্যয়, স্কেলেবিলিটির সমস্যা এবং দীর্ঘ লেনদেন-যাচাইকরণ সময় বাস্তবায়নের ক্ষেত্রে গুরুত্বপূর্ণ চ্যালেঞ্জ সৃষ্টি

© Santiniketan Sahityapath

করতে পারে। এছাড়া বিভিন্ন দেশের আইনগত কাঠামো, তথ্য সুরক্ষা নীতি এবং ব্যক্তিগত গোপনীয়তা (Privacy) সংক্রান্ত বিধিনিষেধ ব্লকচেইনের ব্যাপক ব্যবহারকে প্রভাবিত করতে পারে।

চতুর্থত, বর্তমান গবেষণায় কর্মক্ষমতা বিশ্লেষণ (Performance Benchmarking), অন্যান্য ব্লকচেইন প্ল্যাটফর্মের সঙ্গে তুলনামূলক মূল্যায়ন এবং বাস্তব ব্যবহারকারীর উপর পরীক্ষামূলক যাচাই অন্তর্ভুক্ত করা হয়নি। ভবিষ্যৎ গবেষণায় Hyperledger Fabric, Ethereum অথবা অন্যান্য Permissioned Blockchain Platformএ একই নিরাপত্তা কাঠামোর বাস্তবায়ন, নিরাপত্তা বিশ্লেষণ, কর্মক্ষমতা মূল্যায়ন এবং বৃহৎ পরিসরের সামাজিক তথ্য ব্যবস্থায় এর কার্যকারিতা পরীক্ষা করা হবে।

উপরোক্ত সীমাবদ্ধতা সত্ত্বেও, বর্তমান গবেষণাটি সামাজিক তথ্যের নিরাপত্তা নিশ্চিত করার জন্য একটি সমন্বিত ব্লকচেইন-ভিত্তিক নিরাপত্তা কাঠামোর ধারণাগত ভিত্তি (Conceptual Foundation) প্রদান করে, যা ভবিষ্যতে আরো বিস্তৃত গবেষণা ও বাস্তবায়নের জন্য একটি কার্যকর ভিত্তি হিসেবে বিবেচিত হতে পারে।

সারণি ২: গবেষণায় ব্যবহৃত প্রযুক্তির ভূমিকা

প্রযুক্তি	গবেষণায় ভূমিকা	বাস্তবায়িত হয়েছে
Hyperledger Fabric	সাহিত্য ও তাত্ত্বিক আলোচনা	না
Ethereum	সাহিত্য ও তাত্ত্বিক আলোচনা	না
Python Prototype	পরীক্ষামূলক বাস্তবায়ন	হ্যাঁ
SHA-256	হ্যাশ অ্যালগরিদম	হ্যাঁ

৯. উপসংহার এবং ভবিষ্যৎ গবেষণার দিকনির্দেশনা

বর্তমান গবেষণায় সামাজিক তথ্যের নিরাপত্তা নিশ্চিত করার জন্য একটি ব্লকচেইন-ভিত্তিক নিরাপদ তথ্য ব্যবস্থাপনা কাঠামো প্রস্তাব করা হয়েছে। গবেষণায় প্রথমে সামাজিক তথ্যের নিরাপত্তা-সংক্রান্ত প্রধান সাইবার হুমকিসমূহ বিশ্লেষণ করা হয়েছে এবং পরবর্তীতে ব্লকচেইনের ক্রিপ্টোগ্রাফিক বৈশিষ্ট্য, ডিস্ট্রিবিউটেড লেজার এবং হ্যাশ-ভিত্তিক অখণ্ডতা যাচাইকরণ প্রক্রিয়ার সমন্বয়ে একটি নিরাপত্তা মডেল উপস্থাপন করা হয়েছে। প্রস্তাবিত কাঠামোর কার্যকারিতা প্রদর্শনের জন্য Python-ভিত্তিক একটি Proof-of-Concept Blockchain Prototype তৈরি করা হয়েছে। পরীক্ষামূলক ফলাফল নির্দেশ করে যে প্রতিটি তথ্য ব্লকে SHA-256 হ্যাশ সংরক্ষণ এবং পূর্ববর্তী ব্লকের সঙ্গে ক্রিপ্টোগ্রাফিক সংযোগের মাধ্যমে তথ্যের অখণ্ডতা, ট্রেসেবিলিটি এবং পরিবর্তন-প্রতিরোধ ক্ষমতা নিশ্চিত করা সম্ভব। কোনো তথ্য পরিবর্তিত হলে হ্যাশ যাচাইকরণ প্রক্রিয়ার মাধ্যমে সেই পরিবর্তন তাৎক্ষণিকভাবে শনাক্ত করা যায়।

উল্লেখ্য, বর্তমান গবেষণায় Hyperledger Fabric অথবা Ethereum Frameworkএ পূর্ণাঙ্গ বাস্তবায়ন করা হয়নি। এই গবেষণায় Python-ভিত্তিক প্রোটোটাইপ কেবল প্রস্তাবিত নিরাপত্তা কাঠামোর কার্যকারিতা প্রদর্শনের জন্য ব্যবহৃত হয়েছে। ভবিষ্যৎ গবেষণায় Hyperledger Fabric, Ethereum অথবা অন্যান্য Permissioned Blockchain Platformএ একই কাঠামোর বাস্তবায়ন, কর্মক্ষমতা মূল্যায়ন, স্কেলেবিলিটি বিশ্লেষণ এবং বাস্তব সামাজিক তথ্য ব্যবস্থায় প্রয়োগের সম্ভাবনা নিয়ে গবেষণা করা হবে। গ্রিন ব্লকচেইন প্রযুক্তি ভবিষ্যতের একটি টেকসই সমাধান। প্রযুক্তিগত উন্নয়ন, নীতি সহায়তা এবং জনসচেতনতার মাধ্যমে এটি পরিবেশবান্ধব ও অর্থনৈতিকভাবে লাভজনক উভয় দিকেই গুরুত্বপূর্ণ ভূমিকা রাখতে পারে। লাইটওয়েট ব্লকচেইন প্রযুক্তির উন্নয়ন, হাইব্রিড কনসেনসাস অ্যালগরিদম, ব্লকচেইনে কৃত্রিম বুদ্ধিমত্তার ইন্টিগ্রেশন ভবিষ্যৎ গবেষণার দিকনির্দেশনা হতে পারে।

তথ্যসূত্র:

1. Chen, X., Zhang, X., Wang, Z., Yu, K., Kam-Kwai, W., Guo, H., & Chen, S. (2024). Visual analytics for security threats detection in Ethereum consensus layer. Journal of Visualization, 27 (3), 469–483, https://doi.org/10.1007/s12650-024-00969-z

© Santiniketan Sahityapath

2. Farsi, A. Al, Khan, A., Mughal, M. R., & Bait-suwailam, M. M. (2025). Privacy and Security Challenges in Federated Learning for UAV Systems : A Systematic Review. IEEE Access, PP, 1, https://doi.org/10.1109/ACCESS.2025.3570538
3. Ghosh, S. (2025). A Novel Framework for Financial Cybersecurity and Fraud Detection Using XAI-RNN-SGRU. IEEE Access, PP, 1, https://doi.org/10.1109/ACCESS.2025.3570216
4. Hua, B., Wang, Z., Meng, J., Xi, H. Y., & Qi, R. L. (2023). Big data security and privacy protection model based on image encryption algorithm. Soft Computing, 4, https://doi.org/10.1007/s00500-023-08548-4
5. Li, P., & Zhang, L. (2025). Application of big data technology in enterprise information security management. Scientific Reports, 15(1), 1–15, https://doi.org/10.1038/s41598-025-85403-6
6. Poltavtseva, M. A., Zaitseva, V. V., & Ivanov, D. V. (2024). Assessing the Security of Big Data Systems. Automatic Control and Computer Sciences, 58(8), 1352–1364, https://doi.org/10.3103/S0146411624701025
7. Samanta, A. K. (2021). Blockchain Blended Supply Chain for Improved Operational Management. International Journal of Research, 7(II), 67–78
8. Samanta, A. K., & Chaki, N. (2023). A Game-Based Approach for Mitigating the Sybil Attacks on Blockchain Applications. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 14164 LNCS, 108–123, https://doi.org/10.1007/978-3-031-42823-4_9
9. Samanta, A. K., & Sarkar, B. B. (2021). An Application of Block Chain in Examination System, A Case Study. Advances in Intelligent Systems and Computing, 1178, 109–124, https://doi.org/10.1007/978-981-15-5747-7_8
10. Sinha, P., Rai, A. K., & Bhushan, B. (2019). Information Security threats and attacks with conceivable counteraction. 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies, ICICICT 2019, 1208-1213, https://doi.org/10.1109/ICICICT46008.2019.8993384
11. Zhang, Y., Yang, Y., Chen, Z., Wu, Z., Chen, T., Li, J., Yang, J., Xu, G., Liu, W., Zhang, X., Li, J., Jiang, Y., & Su, Z. (2025). A Practical DoS Attack on Commercial UWB Ranging Systems. IEEE Transactions on Mobile Computing, PP (8), 1-16, https://doi.org/10.1109/TMC.2025.3569972
12. Zhu, M., & Wang, J. (2025). A Trusted Data Access and Transmission Method under Internal and External Threats in the Space Information Network. CFIMA 2024 - Proceedings of 2024 2nd International Conference on Frontiers of Intelligent Manufacturing and Automation, 566–571, https://doi.org/10.1145/3704558.3705531

—

© Santiniketan Sahityapath