Anusandhanvallari
Vol 2025, No.1
July 2025
ISSN 2229-3388

Comparative Study of Traditional vs Blockchain-Based Cybersecurity Approaches

[1]Swati Patil, [2]Smita Chaudhari, [3]Sonal Patil

[1]Asst Professor, CSE dept, G. H. Raisoni College of Engineering and Management, Jalgaon.
swatipatil250178@gmail.com

[2]Associate Professor, Computer Engineering Department, Marathwada Mitra Mandal College of Engineering, Pune

[3]Asst Professor, CSE Department, G. H. Raisoni College of Engineering and Management, Jalgaon.

Abstract: With the expanding digital infrastructures and the rise of increasingly sophisticated cyber threats, there is a growing need for Cybersecurity. For many decades classic cybersecurity implementations (like firewalls, IDS, detection systems, centralized authentication protocols) have formed the foundation for digital defense. But these ways have limitations such as single points of failure, poor transparency and susceptibility to advanced persistence threats. Due to these challenges, blockchain technology has evolved as a suitable solution because of its characteristics of decentralized, immutable, and transparent architecture. In this paper, we compare traditional cybersecurity approach with blockchain-based cybersecurity approach by discussing strengths, weaknesses and areas of use of each approach. Evaluation of parameters — Data integrity, Scalability, Access control, Detection of threats, Anti-fragility against attacks, Among these key parameters, the advantages of both paradigms are emphasized as a trade-off between each other. The paper investigates the impact of blockchain on trust, auditability, and distributed defence in the context of case studies and recent advancements in mainstream application fields such as finance, healthcare, and IoT networks. Results show that though foundational security will always depend on classical ideas, combat systems based on blockchain will bring higher resilience and most notably, trust, in cyber-war setting. Our comparative analysis can help researchers and practitioners who look for hybrid or blockchain-augmented cybersecurity solutions in the transforming digital world.

Keywords: Cybersecurity, Traditional cybersecurity approaches, Blockchain technology.

1. Introduction

Our world is hyper-connected these days and digital technologies have become intertwined with our lives in almost every area. The digital transformation has brought a level of efficiency and convenience into everything from personal communications and financial transactions to essential infrastructure and industrial processes. Yet, the increasing dependence on digital platforms has also beard a larger attack surface, and cyber security has become a key part of information and communication technology in modern times. Cybersecurity has traditionally focused on reactive architectures, e.g., firewalls, antivirus systems, IDS (Intrusion Detection Systems), and centralized authentication frameworks, to detect, prevent, and respond to cyber threats. These systems were built primarily with environments where data lived in secure, central locations and network boundaries were well defined.

With the arrival of cloud computing, Internet of Things (IoT), Mobile technologies, and decentralized applications, digital ecosystems expanded, but traditional cybersecurity models could not keep up. Although foundational, these models are plagued by structural vulnerabilities in the form of single points of failure, citizen trust and data integrity challenges, and limited scalability to a distributed network of MaaS providers. In addition to SMEs being targets for some of the most advanced cyberattacks — the ones that target technology and human weaknesses — the shift in working conditions has made security architecture a more urgent question. This has opened the door to new technologies, with blockchain technology being one of the leading contenders to complement, and in some cases, edge out traditional cybersecurity technologies.

1.1 Importance of Cybersecurity in the Digital Era

Cybersecurity is no longer a domain of IT departments, it is now a national security issue, an economic issue, a corporate governance issue, and of course a personal privacy issue. Data is the new oil equivalent and protecting your data against unauthorized access, alteration, or destruction is paramount in the digital economy. Be it from fraud on financial data, patient data in the healthcare system, or operational continuity of power grids, the trust and functionality of digital infrastructure would come at the cost of cybersecurity.

Today technology now enables organizations and governments alike to be the target of a wide range of cyber incidents——data breaches, ransomware, identity theft, state-sponsored espionage, and sabotage [3]. Incidents like these will cost far more than money: the damage done to a brand's reputation the legal liability and fallout, not to mention the loss of consumer faith can have ripple effects for a long time to come. Top of the list is the current impact of cybercrime; in the latest reports, global cost of cybercrime is expected to increase over \$10 trillion dollars per year by 2025. These threats have elevated cybersecurity to strategic importance across sectors, leading to investment in human capital as well as technology.

Additionally, regulations like General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) as well as Cybersecurity Maturity Model Certification (CMMC) have put far more stringent compliance requirements, leading to a rise in need for data protection methods that are secure, transparent, easy-to-understand, and auditable. Thus, the significance of cybersecurity in this age is more than just protecting the technical ecosystem but also in the context of compliance, business continuity, and consumer trust.

1.2 Overview of Rising Cyber Threats and Evolving Attack Vectors

An active war has caused the cyber threat landscape to grow more complex and multidimensional. The earliest threats were rather basic, often consisting of viruses and worms with restricted goals. Today, cyber threats are a lot more complex, using cutting-edge technologies like AI, machine learning, and social engineering to carry out targeted and long-lasting attacks. Threat actors can be individual hackers, organized cybercriminal groups, state-sponsored entities, and hacktivist organizations.

Today's attack vectors make use of software bugs, human error, supply chain weaknesses and network misconfigurations. Some of the most common and dangerous threats include:

- Ransomware: Malicious software that encrypts files and demands payment for decryption keys.

- Phishing and Social Engineering: Manipulative tactics used to deceive individuals into revealing sensitive information.
- Distributed Denial of Service (DDoS) Attacks: Overwhelming network resources to disrupt services.
- Advanced Persistent Threats (APTs): Long-term, targeted attacks designed to steal data or compromise systems without detection.
- Zero-Day Exploits: Attacks that target previously unknown vulnerabilities before patches are available.

In addition, the rise of IoT devices and remote work has introduced new vulnerabilities that are difficult to manage using traditional perimeter-based defenses. As cyberattacks grow more intelligent and persistent, static security models are increasingly inadequate, prompting the need for dynamic, adaptive, and resilient security solutions.

1.3 Motivation for Exploring Alternative Approaches like Blockchain

Given the limitations of traditional cybersecurity systems—especially in dealing with decentralized environments and advanced threat actors—there is a growing interest in exploring novel approaches that can provide enhanced security guarantees. Blockchain technology, originally developed as the foundation of cryptocurrencies like Bitcoin, has demonstrated key properties such as immutability, decentralization, and consensus-based validation that are highly desirable in security contexts.

Blockchain's ability to record transactions in a tamper-proof, transparent, and distributed ledger offers a new paradigm for securing data and digital interactions. Unlike traditional systems where a central authority controls access and logging, blockchain distributes trust across a network of nodes, making it inherently resistant to single points of failure and unauthorized manipulation. These properties have fueled research and development into blockchain-based applications for secure data sharing, identity management, access control, and auditability.

The motivation for incorporating blockchain into cybersecurity lies in its potential to:

- Eliminate the need for trusted third parties.
- Create immutable logs for traceability and compliance.
- Enable decentralized identity frameworks to prevent credential theft.
- Enhance the integrity and availability of critical data and services.
- Facilitate secure peer-to-peer communications in IoT and edge networks.

As organizations seek to modernize their security posture, blockchain offers a compelling supplement—or even an alternative—to legacy security infrastructures.

1.4 Objectives and Scope of the Comparative Study

This study aims to perform side-by-side comparison between traditional cyber security approaches against a block chain based security model. The goal is to discern both the resilience and fragility of each type of reasoning, as well as the specific circumstances when one outperforms the other. The objective of developing this comparative analysis is to outline a comprehensive and balanced perspective on the two paradigms, facilitating decision making both in academic research as well as practical implementation, by evaluating such paradigms against key dimensions including data immutability, event detection, event scalability, event auditability, and event robustness.

This comparative study focuses on:

- Defining and contextualizing traditional and blockchain-based cybersecurity approaches.
- Analyzing their performance in handling modern cyber threats.
- Highlighting real-world use cases and applications.
- Identifying integration challenges and hybrid model opportunities.
- Recommending best practices for future cybersecurity frameworks.

The scope includes a review of existing literature, comparative analysis through defined metrics, and insights into emerging trends and technologies. It also covers sector-specific use cases in areas such as healthcare, finance, and the critical infrastructure, where the security, transparency, and scalability needs compelled by industry-specific requirements are high. In the final analysis, this research aims to fill the knowledge gap between traditional cybersecurity approaches and next generation approaches and aid the decision makers in the dynamic landscape of cybersecurity.

2. Literature Review

Akbar M et al. 2024 [1] A blockchain-based trust model for providing secure data transmission over the cloud computing, exploiting a multi-risk protection scheme comprising of quantum key distribution (QKD), Merkle-tree based integrity checks and a Modified Advanced Encryption Standard (MAES), all embedded into the blockchain. Through experiments that involve simulating a specific cloud data transport scenario, we exemplify the cloud computational/storage overhead reduction (~25% compared to SVPAC, ~36% compared to CP-ABE), data integrity and security improvement as well.The results show the model outperforms baseline schemes in efficiency and robustness while enabling tamper-resistant logging and trust in transmission.

Mazhar T. et al. (2023) [2] conducted an analysis of cybersecurity attacks and solutions in smart grids using machine learning (ML) techniques and blockchain methods. They reviews a taxonomy of attacks on smart grid layers—users, sensor communications, and network administrators—and surveys state-of-the-art ML-based detection and blockchain-based mitigation strategies. Though no new dataset is introduced, the authors discuss existing case studies and deployed solutions. They conclude that combining ML for threat detection with blockchain for secure data sharing can significantly improve resilience, though they note a need for clearer methodological detail in the AI components.

Choudhary D et al. (2022) [3] proposeed a blockchain-enabled cybersecurity framework for connected networks, detailed in Peer-to-Peer Networking and Applications. The method emphasizes peer-to-peer data management and cloud storage security, proposing a TOPSIS-based RSU (Roadside Unit) priority scheduling scheme (TRP) that integrates blockchain ledger entries for secure transaction logging and access control. Though the author does not mention a public dataset, simulations illustrate how TRP improves scheduling fairness and prevents unauthorized access in connected vehicular or sensor networks. The framework demonstrates enhanced decentralization and auditability while reducing latency and overhead.

Yadav S.K. et al. (2022) [4] included a real–time synergistic blockchain–based cyber security solution providing an extra layer on top of existing frameworks (Multimedia Tools and Applications). Their approach involves Cyber-Soldiers, fully automated agents that write to the blockchain module according to the outputs of an artificial neural network (ANN). Experimental evaluation which is done through simulations of network traffic and metrics like packet drop ratio (PDR) and detection rate. The results yielded better resilience and adaptability: integrated design and legacy systems have been able to reduce a significant amount of dropped packets and as well as increase the time it takes to detect anomalies indicating responsive benefits for both detection and response to anomalies.

Ragab M et al. Replication: In [5] proposed a deep learning-based architecture (BDLE-CAD) to secure critical infrastructures and industrial control models. It involves attracting ECOA-FS (chimp optimization) feature selector, a search and rescue algorithm (SAR) employed for building deep neural network (DNN) for intrusion detection, as well as Blockchain-entitled Integrity Checking Scheme (BEICS) for protecting against misrouting attack. Evaluated using simulated ICS datasets, their model achieves ~92.6% detection accuracy, outperforming baseline IDS frameworks, and ensures immutable logging and secure edge service management.

Fahmi N. et al. (2022) [6] carried out a comparative analysis of blockchain applications and security challenges, tracing development from Bitcoin to cybersecurity domains. They review blockchain's technical principles—consensus protocols, cryptographic schemes—as well as vulnerabilities including privacy leaks, scalability issues, and smart contract risks. No empirical dataset is used; the work is a systematic literature review. The authors synthesize findings from existing studies to highlight key security threats, applications, and open research gaps, concluding that while blockchain enhances privacy, transparency, and integrity, it faces limitations in throughput, regulation, and attack resilience.

S. Rathore et al. (2021) [7] is designed a DeepBlockNet for the next-generation implementations of Industrial Cyber-Physical Systems (CPS) based on blockchain-based deep learning framework. Their approach decentralizes AI operations and eliminate central trust using edge-deployed DL models integrated with a blockchain layer. It uses CPS/IoT data simulations for evaluation under two metrics: detection accuracy and latency. The results show that their method is able to achieve higher detection performance and great accuracy of models without the effect of single-point control vulnerabilities, which further confirms the effectiveness of the method in decentralized and secure CPS environments.

Kane J. Smith et al. (2020) [8] They used Value—Focused Thinking (VFT), a multi—objective decision analytic technique, to model organizational—level objectives, which can be mapped to high and low security outcomes, to evaluate the potential contribution of blockchain to cybersecurity in respect to financial transactions. Unlike the two prior papers, they do not include an experimental dataset, but apply VFT to assess chain solutions against strategic needs such as ensuring confidentiality, integrity, and having no higher costs than ever. Although they determine that

blockchain has the potential to greatly increase trust and decrease the potential for fraud very intricate and accurate evaluation frameworks will be needed to synthesise and meaningfully compare various implementations of the technology within financial operations.

O. Abdulkader et al. (2019) introduced a lightweight cyber security architecture for IOT ecosystem on blockchain, well-structured in modular form with Edge Block Manager (EBM), Aggregation Block Manager (ABM), and Cloud Block Manager (CBM). This design optimize the resource overhead during IoT transaction security. In the synthetic IoT traffic simulations, using a discounted transaction cost and lower latency / transaction overhead enabled better data accessibility and integrity as well as lower data stewardship cost. The framework works at all with minimal requirements, providing a tamper-proof logging mechanism suitable for resource-limited settings, without too much computation [9].

J. White et al. (2019) [10] Their model is continuous and utilize a blockchain for continuous management of security policies and security logs. Their approach imagines a use case where blockchain enables real-time policy updates, immutable audit trails, and automated governance. The paper details system flow and managerial benefits rather than datasets, and is intended to serve as a conceptual or prototype framework rather than empirical study with future research on those empirical study dimensions to follow some years later. Their claim is that blockchain can overcome static, linear approval workflows in traditional cybersecurity operations, thereby enabling improved responsiveness and visibility within enterprise contexts.

A. Rot et al. (2019) [11] explored blockchain's dual potential in cybersecurity, conceptualizing both defensive and offensive uses of blockchain-based platforms. They map solutions across dimensions of whether blockchain is the target or a means to an end, identifying threat types such as wallet, network, smart contract, and consensus vulnerabilities. Their method involves a structured framework analysis rather than empirical datasets—classifying over 30 attack vectors and categorizing blockchain solutions accordingly. They conclude that although blockchain offers strong defensive benefits—such as immutable logs, identity verification, and distributed trust—it also introduces novel attack surfaces. The study cautions that whether blockchain adoption leads to net security gains depends on careful mitigation of those platform-specific risks.

Malomo O.O et al. (2018) [12] presented BFC² (Blockchain-Enabled Federated Cloud Framework), which integrates blockchain with federated cloud systems to secure offsite digital asset storage. Their architecture comprises Block Vault, Block Generator, and Threatroscope modules. Access control employs multi-factor authentication, split-knowledge, and hardware fingerprints; logging is distributed and immutable. Evaluated using simulations of federated cloud environments with synthetic workloads, the framework demonstrates improved data integrity, scalability, and breach detection, outperforming traditional storage systems in monitoring unauthorized access and reducing transaction overhead. The proof-of-concept shows enhanced privacy, accountability, and early breach detection in federated settings.

Table 2: Comparative Analysis of Literature Reviews

Author name & ref no.	Methodology Used	Datasets used	Advantages	Results
Akbar et al. [1]	Blockchain trust model with multi-risk protection (QKD, MAES, Merkle tree)	Simulated cloud data scenarios	Improved integrity, reduced overhead, trust in cloud transmission	25â€“36% lower overhead than baselines
Mazhar et al. [2]	Machine learning and blockchain methods for smart grid	Reviewed smart grid case studies	Enhanced threat detection and secure data sharing	Conceptual results; improvement noted in resilience
Choudhary & Pahuja [3]	TRP: Blockchain with TOPSIS-based RSU prioritization	Simulated vehicular/sensor network	Fair resource scheduling, access control, low latency	Improved scheduling and reduced delay
Yadav et al. [4]	Cyber Soldiers + ANN integrated with blockchain	Simulated network traffic	Dynamic threat detection, reduced packet drops	Improved detection and network performance
Ragab & Altalbe [5]	BDLE-CAD architecture with ECOA-FS, DNN, BEICS	Simulated ICS datasets	High accuracy, lightweight logging, real-time alerts	92.6% accuracy, better than standard IDS
Fahmi et al. [6]	Comparative analysis of blockchain applications and risks	No dataset (literature-based)	Highlights evolution, risks, and gaps in blockchain cybersecurity	Synthesized comparative insights
Rathore & Park [7]	DeepBlockIoTNet: Blockchain-based DL for CPS	Simulated CPS data	Decentralized AI security, trustless detection	High detection accuracy and latency reduction
Smith & Dhillon [8]	Value-Focused Thinking for blockchain in finance	No empirical dataset	Decision model for assessing blockchain vs. traditional	Improved fraud risk control potential
Abdulkader et al. [9]	EBM + ABM + CBM layered blockchain for IoT	Synthetic IoT traffic	Lightweight logging, access control	Lower latency, energy-efficient security
White & Daniels [10]	Real-time policy mgmt. through blockchain	No dataset (conceptual)	Immutable logging, continuous audit	Conceptual benefits to policy oversight
Rot & Blaicke [11]	Framework analysis of blockchain attack/defense use	No dataset (taxonomy-based)	Defensive and offensive insights on blockchain roles	Mapped over 30 attack vectors
Malomo et al. [12]	BFCÂ²: Blockchain-enabled federated cloud security	Simulated federated cloud workloads	Scalable logging, early breach detection	Improved scalability and audit performance

The table 1, provides a comprehensive comparative analysis of twelve blockchain-based cybersecurity research papers. It summarizes the approaches, benchmarks, benefits, and findings of each work providing an overview of approaches

towards improving cybersecurity in different areas. This systematic comparison will help point ways to trends, strengths, and gaps in the new domain.

3. Traditional Cybersecurity Approaches

3.1 Core Components of Traditional Cybersecurity

Conventional cyber security is dependent on foundational tools and mechanisms that are built to prevent, detect and respond/counter cyber threats. Used in conjunction, these tools create a layered defense strategy commonly known as "defense in depth." Firewalls, anti-malware, intrusion detection/prevention systems (IDS/IPS), passwords and 2FA, centralized authentication and authorization methods are among the most commonly used and integral components.

- Firewalls: The firewall is network security device/software that monitors and controls incoming and outgoing network traffic. In essence, it sits between trusted internal networks and untrusted external networks, such as the internet. Nowadays, most of the firewalls are able to block unauthorized access to the network or a processor device, and also allow the normal communication over the Internet, it operates at multiple layers of the network stack e.g. Packet filtering, Stateful inspection, and others. Firewalls can be hardware- or software-based or even be provided as a cloud service, and each has its own use cases.

- Antivirus Software: Antivirus software is software that is used to prevent, detect, and remove malicious software (malware), such as viruses, worms, trojans, ransomware and spyware. These programs operate by using signature based detection to identify known threats and heuristic analysis to flag behavior that seems suspicious. Some modern antivirus even use machine learning and behavioral analytics for zero-day threat identification.

- Intrusion Detection and Prevention Systems (IDS/IPS): IDS and IPS are key components for monitoring and threat detection in a network. While a IDS monitors and raises alerts on invasive activity, an IPS takes it one notch forward in that it also attempts to block all currently detected threats within a minimum period of time. Detection methodology-based, these systems can be signature-based, anomaly-based, or hybrid. Your IDS/IPS can get visibility into your network behavior and can help block some attacks, but IDS/IPS can have false positives and cannot always analyze encrypted or obfuscated traffic.

- Centralized Authentication and Access Control: Authentication and authorization are necessary, so only authorized users can access certain systems or information. Methods of authentication used in most systems today primarily depend on username-password pairs, which can easily be exploited via brute-force attacks, phishing, and credential stuffing. For better security, several systems now enforce two-factor authentication (2FA) or multi-factor authentication (MFA), which demand additional authentication once the password has been entered − the OTP, a biometric scan, or a security token.

Most of the centralized access control systems follows a model such as Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) which means that permissions governance is done by a central system. Centralized systems, while great for control and visibility, can lead to single points of failure and limited scaling in very distributed or dynamic environments.

These core components are the foundation of the traditional cybersecurity architectures. Although they are still critical to many operational environments, the rise of advanced cyber threats and the ability to build highly decentralized network models have shown weaknesses that new technologies such as blockchain attempt to fill.

3.2 Techniques and Protocols

Conventional cybersecurity employs multiple cryptographic methods and protocols to secure/assure transactions and secure communication (including anonymous communication), and to provide data confidentiality, data integrity, and authentication. Public Key Infrastructure (PKI), Virtual Private Networks (VPNs), SSL/TLS protocols, and hashing algorithms are only some of the most widely use standards.

- PKI: PKI describes a system utilizing asymmetric encryption (public-private key) over a network. The system grants secure data exchange, electronic signatures, and identification. So for example, A want to send a message to B in an encrypted way, A uses B public key to encrypt the message. Then B decrypts it with their private key. For instance, one of the most prevalent PKIs, RSA algorithm uses:

$$\text{Encryption: } C = M^e \ mode \ n,$$

$$\text{Decryption: } M = C^d \ mode \ n$$

- VPNs: VPNs build tunnels of encryption over the internet, securing data in transit between servers and users. Protocols such as IPsec or OpenVPN are used to thwart efforts to listen in on conversations or to perform man-in-the-middle (MITM) attacks.
- SSL/TLS protocols: It makes web communication more secure by establishing an encrypted link between browser and server by means of symmetric and asymmetric cryptography. It ensures authentication, confidentiality, and integrity of data.
- Hashing algorithms: A hashing algorithm, for example, SHA-256 (hash function), will output a hash of a fixed length that uniquely identifies the input data. They are employed to ensure data integrity and to securely store passwords. For example:

$$SHA-256(input) \rightarrow 64-character\ hexadecimal\ hash$$

These protocols are vital to traditional cybersecurity systems but can be limited in trust decentralization and auditability.

3.3 Limitations

Traditional cybersecurity systems, while foundational to digital protection, are increasingly facing limitations in the face of modern threats and distributed architectures. The table 2 below highlights key challenges associated with these conventional approaches, particularly in terms of trust, scalability, and resilience.

Table 2: limitations of traditional cybersecurity approaches

Limitation	Description
Single Point of Failure	Centralized systems rely on a main server or authority; if compromised, the entire system becomes vulnerable or non-functional.
Scalability Challenges	Traditional architectures struggle to efficiently scale with large numbers of users, devices (e.g., IoT), or geographically distributed systems.
Insider Threats and Lack of Transparency	Security mechanisms often lack full traceability, making it easier for insiders to abuse access without immediate detection or accountability.
Difficulties in Auditability and Data Integrity	Centralized logs and mutable databases can be altered or deleted, making it hard to verify event history or ensure data hasn't been tampered with.

4. Blockchain-Based Cybersecurity Approaches

4.1 Core Principles of Blockchain-Based Cybersecurity Approaches

The Blockchain Technology provides us with some basic principles which can be great substitutes for the conventional cybersecurity mechanisms. This is why blockchain, with its security architecture based on four fundamental principles (decentralization, immutability, transparency and consensus mechanisms) is becoming increasingly important for the development of new cybersecurity applications.

- Decentralization: Decentralization lies at the very core of blockchain, meaning no central authority is required for data management, access control, or transaction validation. It is an information system that breaks down information into smaller pieces and disperses it to everyone through a network (each node has a copy of the ledger). Such an architecture minimizes the likelihood of a single point of vulnerability, which is a flaw found in legacy centralized and trigger box systems. By decentralizing, you also improve fault tolerance and resilience since an attacker would have to breach most of the nodes to attack the entire network.

- Immutability: This means that data written on the blockchain is immutable, so once recorded it is not possible to change or delete it without consensus among the network. Every block is tied to the previous one cryptographics, creating securely linked records. The ability to not alter any data is fed to it and is also one of the keys to keeping the data truthfulness and transparency. Immutability in Cybersecurity Immutability facilitates secure, traceable, and auditable logging of system events for more straightforward detection and investigation of malicious activities.

- Transparency: Because of its transparent nature, all participants within the network have access to a version of the ledger that has been verified and synchronized across the nodes. Public blockchains are completely open and even anyone can see the entire transaction (but never private information), while permissioned blockchains keep some level of secrecy under control, and thus are more suitable for enterprise use. The transparency also contributes to ensure accountability and trust among the users and other stakeholders. Transparent access logs and transactional histories help identify malicious behavior, aiding in regulatory compliance in cybersecurity.

- Consensus Mechanisms: Consensus Mechanisms Consensus mechanisms are protocols that allow for the agreement between different distributed nodes regarding the state of the blockchain. Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) are some of the algorithms that validate transactions, giving them their validity without having a central authority. Such mechanisms are crucial for preventing tampering with data and sustaining network integrity, particularly in hostile conditions.

All these principles combined, make blockchain a very strong base on which to build secure, transparent, and more resilient cyber security solutions, especially in decentralized environments (IoT, supply chains, and cloud computing).

4.2 Technologies Used

The use of blockchain cybersecurity uses several technologies to provide better data protection, integrity, and trust among stakeholder parties in a decentralized system. These include smart contracts, cryptographic hashing, and distributed ledgers, which are integral to the reshaping of modern cybersecurity architectures.

- Smart Contracts: Smart contracts are programs that live on the blockchain and that automatically enforce rules and agreements when certain conditions are met, thanks to the self-executing feature of the program. Smart contracts make unnecessary the involvement of intermediaries whilst also limiting the risk of manipulation or human error. In the field of cybersecurity, implementation of smart contracts is able to automate identity verification, access control, and incident response processes. A smart contract can be utilized that improves security and transparency by automatically granting or revoking access to digital assets depending on user behavior (for example, if the user has ever lost a digital asset or buys NFTs).
- Cryptographic Hashing: Data integrity and authentication of the data provided within the blockchain are guaranteed with cryptographic hashing. A hash function converts arbitrary length data into a fixed size alphanumeric characters (hash value), and it completely changes by the slightest change in input. Transactions are secured and blocks are linked using common algorithms such as SHA-256. It is also tamper-evident, which makes unauthorized data changes easy to detect.
- Distributed ledgers: It keeps a record of all transactions over a variety of nodes, no longer having a centralized problem point. Each node holds a copy of the ledger, and the ledger can only be updated when it meets consensus. Such decentralization not only makes the system more resilient but ensures that no one can tinkerer with the data while also establishing a transparent trail to know who/where it has come from.

Together, these technologies form the backbone of blockchain-based cybersecurity, enabling secure, decentralized, and verifiable systems ideal for modern digital environments.

4.3 Application and Benefits

Blockchain-based cybersecurity solutions leverage specific applications to address key challenges in digital security. The table 3 below outlines these applications along with their associated benefits, demonstrating how blockchain enhances trust, resilience, and control across various domains.

Table 3: Applications and Their Associated Benefits

Application	Associated Benefits
1. Decentralized Identity Management	- Eliminates dependency on centralized authorities. - Enhances privacy and reduces identity theft.
	- Gives users full control over their digital identities.
2. Secure Data Sharing & Access Control	- Only authorized entities can access data. - Access policies are enforced automatically via smart contracts.
	- Prevents unauthorized changes or data leaks.
3. Tamper-Proof Logging & Audit Trails	- Ensures data integrity and immutability. - Enables transparent and real-time auditing.
	- Helps meet compliance and regulatory standards.
System-Wide Advantages	- Improved trust across all participants. - Increased resilience to cyberattacks. - Stronger IoT/cloud protection.

5. Comparative Analysis

The differences in architecture, behavior, and flexibility between the cybersecurity systems in traditional method and the blockchain cybersecurity approach. Traditional systems are centralized, which makes it easier to manage, but also increases the risk of single points of failure and insider attacks. Introduced and practised widely, their authentication mechanisms like passwords and 2FA are susceptible to phishing attacks and credentials theft. Traditional systems rely on log files, which can be manipulated without adequate safeguards, to ensure data integrity and limit auditability.

Conversely, a tamper-resistant decentralized model can be built on blockchain. Data stored on the blockchain is immutable and traceable by using consensus mechanisms and cryptographic hashing, resulting in a high degree of trust and integrity. Another key advantage of blockchain is decentralized identity management (DID), which minimizes dependence on central authorities and enhances user control over credentials. But this comes at a cost, in the form of greater complexity to implement, greater difficulty in scaling, as well as compliance challenges, especially in public blockchain settings. Even with these challenges, blockchain promises great resistance to DDoS attacks, strong resiliency features and it offers transparent and verifiable audit trails, are powerful components find appropriate places in the field of cybersecurity.

Table 4: Comparative Analysis of Traditional vs Blockchain-Based Cybersecurity Approaches

Criterion	Traditional Cybersecurity	Blockchain-Based Cybersecurity
Data Integrity & Immutability	Vulnerable to tampering; logs can be altered or deleted	Immutable data storage through cryptographic hashes and consensus
Authentication & Identity Mgmt	Centralized identity systems (e.g., passwords, 2FA)	Decentralized Identity (DID) and public-private key cryptography
Attack Resilience	Focused on perimeter defenses; vulnerable to insider & DDoS attacks	Resilient through decentralization; harder to exploit single point
Scalability & Performance	Mature but limited in large-scale, distributed environments	Still evolving; faces latency and throughput challenges
Auditability & Transparency	Log-based and modifiable; limited visibility	Tamper-proof logs; fully auditable and transparent

Cost & Implementation Complexity	Generally lower initial cost; easier to deploy	Higher development/maintenance cost; integration can be complex
Regulatory Compliance & Privacy	Well-aligned with current regulations; easier access control	Offers transparency, but public chains may pose privacy challenges

The table 4 provides a side-by-side comparison of traditional and blockchain-based cybersecurity approaches across key evaluation criteria. It highlights the strengths and limitations of each method, offering insight into how blockchain can address gaps in traditional systems while also introducing new challenges.

6. Case Studies or Use Cases

6.1 Traditional Cybersecurity: Applications in Enterprise Networks and Government Systems

Legacy cybersecurity mechanisms continue to serve as the backbone of digital security in enterprise and government spaces. Enterprise networks have utilized tools like firewalls, antivirus solutions, IDS/IPS and centralized access control tools to map the organizational IT infrastructure with security. In fact, large enterprises tend to implement the NGFWs along with EPP (endpoint protection platform) solution in order to monitor and prevent threats across thousands of devices. In addition, access security is fortified by the use of solutions like VPNs and MFA in the wake of remote work.

Cybersecurity practices in government systems are dictated by strict standards like the U.S. FISMA (Federal Information Security Management Act) or international standards like ISO/IEC 27001. To illustrate, role-based access to sensitive governmental data, such as tax records, criminal databases, or national IDs, is typically done by government agencies. Logs used for logging and auditing user behavior, although those logs can be tampered with or deleted. These more traditional tools do provide scalability and some integration into legacy infrastructure, but they also typically lack real-time immutability, distributed trust and other elements that have become increasingly essential in the modern threat landscape.

6.2 Blockchain-Based Cybersecurity: Emerging Applications in Key Sectors

When it comes to cybersecurity that is supported by blockchain, we would find that only those sectors that are majorly concerned about data integrity, traceability, and decentralized trust, are moving toward implementation.

Blockchain helps to secure electronic health records (EHRs) in the health sector. Work held in block chain behind projects like MedRec and HealthChain, where patient data is not just available but locked down, such that only those with the right and proper credentials can access it. This improves patient privacy and allows hospitals, insurance providers, and researchers to safely share valuable information. Additionally, smart contracts prevent violations of data protection regulations, like HIPAA simple automating consent management. Blockchain prevents the financial sector from fraud and money laundering as it contains strong mechanisms. They also enable double spends protection using cryptographic validation of transactions, and immutable audit trails for post-incident investigations. Ripple and Stellar networks enable cross-border payments that are visible and can be tracked in real time. In addition, shared, verified identity credentials can improve Know Your Customer (KYC) processes across institutions. Blockchain technology allows traceability of goods from origin to customer in supply chain management. IBM and Walmart, as

well as others, utilize topics such as Blockchain to track food products & number and prevent counterfeit goods, for example. Every event around the supply chain are recorded by one immutable transaction thus allowing real time verification and regulatory compliance.

Since devices are widely distributed and typically resource-constrained in IoT environments, Blockchain provides secure communication and data validation. Using lightweight blockchain protocols integrated with edge computing, it enables secure device registration, firmware updating, and data logging without needing a centralized authority. Blockchain use-cases found in projects like IOTA and Filament can be seen as solutions to securing smart cities and industrial IoT systems.

7. Hybrid Cybersecurity Models

The changing threat landscape and shortcomings of the security-by-design paradigm have driven the need for interest in hybrid cybersecurity approaches that combine the strengths of traditional technologies with the decentralized and incorruptible properties of blockchain. Such integration is not only realistic, but imperative, with organizations looking for solutions that will scale, be agile, and transparent, all of which fall in line with the modern digital infrastructure.

7.1 Combining Strengths of Traditional and Blockchain Methods

Well-established as they are, traditional cybersecurity systems support known mechanisms such as firewalls, intrusion detection/prevention systems (IDS/IPS), antivirus, centralized authentication protocols, etc. These mainly utilize perimeter security and user access level managing and can be trusted in detecting the known threats. Yet they are usually so centralized, audit vulnerable, and insider prone.

Blockchain technology, however, is far superior for data integrity, trustless decentralization, logging immutable events, and peer validation. Although blockchain cannot replace traditional tools, it could augment these tools by securing audit trails, managing decentralized identities, and enabling distributed access control.

Hybrid models attempt to retain the original scalability and manageability of traditional systems while using components from a blockchain stack to improve transparency, trust, and resistance to tampering.

7.2 Examples of Integrated Frameworks for Layered Defense

Several research and industry prototypes have demonstrated successful integration of blockchain with traditional tools:

- SIEM Systems with Blockchain Logging: Security Information and Event Management (SIEM) platforms can integrate blockchain to record alerts and incident logs immutably, preventing tampering during forensic investigations.
- Decentralized Identity + Centralized Access: Blockchain-based Decentralized Identifiers (DIDs) can be used for identity verification, while traditional systems still manage session-based access and permissions using role-based access control (RBAC).
- Smart Contracts in Intrusion Response: Traditional IDS detects anomalous behavior and triggers blockchain-based smart contracts to automate response actions such as isolating infected nodes or revoking access credentials.

- Blockchain-Enhanced VPNs: Traditional VPNs ensure encrypted communication, while blockchain can be used to authenticate users and manage VPN session logs in a transparent, decentralized manner.

These integrated models create a multi-layered defense, improving both proactive and reactive cybersecurity measures.

7.3 Future Research Directions in Hybrid Models

Despite promising progress, hybrid models are still in early stages and present several open research challenges. Future studies should explore:

- Interoperability protocols that facilitate seamless data flow between blockchain and legacy systems.
- Lightweight blockchain implementations optimized for resource-constrained environments like IoT and mobile networks.
- AI-Blockchain integration, where machine learning models assist in dynamic threat detection while blockchain ensures secure model deployment and auditability.
- Scalable consensus algorithms that reduce latency and energy consumption, making blockchain more viable in real-time cybersecurity applications.
- Policy-aware smart contracts that adhere to organizational and regulatory requirements during autonomous threat mitigation.

In conclusion, hybrid cybersecurity models hold immense potential to offer comprehensive, resilient, and transparent protection by leveraging the best of both traditional and blockchain approaches. As research matures, these integrated systems are likely to become the standard for securing complex, decentralized digital ecosystems.

8. Conclusion

By contrasting traditional solutions used in cybersecurity with emerging solutions based on the Blockchain paradigm this comparative study has made the transition in cybersecurity more transparent. Foundational defenses against cyber threats included conventional methods such as firewalls, intrusion detection systems, and centralized authentication protocols. But today, surrounded by crypto giants, centralized control, insider threats and lack of auditability are huge drawbacks in a distributed world. The features of decentralization, immutability, and transparent consensus mechanisms enable foundational transformative solutions using blockchain for cybersecurity. Data integrity, decentralized identity management, and tamper-proof audit trails are a few of these functionalities. Use cases in healthcare, finance, IoT, and supply chain sectors exemplify how blockchain can secure sensitive, distributed, critical digital ecosystems. Nonetheless, scalability, energy use, and regulatory uncertainty must be overcome before mainstream acceptance. It also highlights the potential of hybrid models that combine the reliability of traditional systems with the resilience of blockchain in cybersecurity. They offer a more sophisticated, layered defense model that strengthens threat detection, data protection and response capabilities in real time. Final Thoughts Traditional CyberSecurity is not DeadHybrid & Blockchain based models going to be powerful proceeding models for CyberSecurity with the evolving needs of next generation digital infrastructure. These integrated models need to be refined in terms of ease of use, compatibility, and regulatory approval prior to real-world implementation in future research.

References

[1] Akbar, M., Waseem, M.M., Mehanoor, S.H. et al. Blockchain-based cyber-security trust model with multi-risk protection scheme for secure data transmission in cloud computing. Cluster Comput 27, 9091–9105 (2024). https://doi.org/10.1007/s10586-024-04481-9

[2] Mazhar, T., Irfan, H. M., Khan, S., Haq, I., Ullah, I., Iqbal, M., & Hamam, H. (2023). Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods. Future Internet, 15(2), 83. https://doi.org/10.3390/fi15020083

[3] choudhary, D., Pahuja, R. A blockchain-based cyber-security for connected networks. Peer-to-Peer Netw. Appl. 16, 1852–1867 (2023). https://doi.org/10.1007/s12083-023-01506-9

[4] Yadav, S.K., Sharma, K., Kumar, C. et al. Blockchain-based synergistic solution to current cybersecurity frameworks. *Multimed Tools Appl* 81, 36623–36644 (2022). https://doi.org/10.1007/s11042-021-11465-z

[5] Ragab, M., & Altalbe, A. (2022). A Blockchain-based architecture for enabling cybersecurity in the internet-of-critical infrastructures. *Comput. Mater. Contin,* 72(1), 1579-1592. http://dx.doi.org/10.32604/cmc.2022.025828

[6] Fahmi, N., Hastasakti, D. E., Zaspiagi, D., Saputra, R. K., & Wijayanti, S. (2022). A comparison of blockchain application and security issues from Bitcoin to Cybersecurity. Blockchain Frontier Technology, 2(2), 58–65. https://doi.org/10.34306/bfront.v2i2.231

[7] S. Rathore and J. H. Park, "A Blockchain-Based Deep Learning Approach for Cyber Security in Next Generation Industrial Cyber-Physical Systems," in *IEEE Transactions on Industrial Informatics,* vol. 17, no. 8, pp. 5522-5532, Aug. 2021, doi: 10.1109/TII.2020.3040968. https://doi.org/10.1109/TII.2020.3040968

[8] Kane J. Smith, Gurpreet Dhillon; Assessing blockchain potential for improving the cybersecurity of financial transactions. *Managerial Finance* 29 August 2020; 46 (6): 833–848. https://doi.org/10.1108/MF-06-2019-0314

[9] O. Abdulkader, A. M. Bamhdi, V. Thayananthan, F. Elbouraey and B. Al-Ghamdi, "A Lightweight Blockchain Based Cybersecurity for IoT environments," *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom),* Paris, France, 2019, pp. 139-144, doi: 10.1109/CSCloud/EdgeCom.2019.000-5. https://doi.org/10.1109/CSCloud/EdgeCom.2019.000-5

[10] J. White and C. Daniels, "Continuous Cybersecurity Management Through Blockchain Technology," *2019 IEEE Technology & Engineering Management Conference (TEMSCON),* Atlanta, GA, USA, 2019, pp. 1-5, doi: 10.1109/TEMSCON.2019.8813712.

[11] A. Rot and B. Blaicke, "Blockchain's Future Role in Cybersecurity. Analysis of Defensive and Offensive Potential Leveraging Blockchain-Based Platforms," 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2019, pp. 447-451, doi: 10.1109/ACITT.2019.8779855. https://doi.org/10.1109/ACITT.2019.8779855

[12] Malomo, O.O., Rawat, D.B. & Garuba, M. Next-generation cybersecurity through a blockchain-enabled federated cloud framework. J Supercomput 74, 5099–5126 (2018). https://doi.org/10.1007/s11227-018-2385-7