BLOCKCHAIN FOR NETWORK SECURITY:

A Comprehensive Study

Anushka Tiwary IT H-229302635

Rishita Jain IT H-229302627

Abstract

Blockchain is a game-changing technology that makes it possible to create dependable applications without requiring peer trust. Blockchain technology establishes worldwide, unchangeable repositories that ensure the integrity and non-repudiation of data that is saved. Furthermore, the difficulty of processing and managing massive amounts of data with ever-lower latencies is increased by the boom in the quantity and availability of data on computer networks. Consequently, machine learning and artificial intelligence techniques advance significantly and become key enabling technologies for next-generation networks. This special edition is devoted to these emerging technologies that are reshaping computer networks globally to become more dependable while also opening up new avenues for distributed and knowledge-based security services and applications. The papers in this issue address a variety of subjects, including new cryptographic models applied to healthcare, intelligent threat-detection systems, and new consensus mechanisms for the blockchain.

Introduction

Blockchain technology has revolutionized the landscape of application development by offering a paradigm shift in creating secure and reliable applications without mandating trust among network participants. Its immutable and global repositories assure data integrity and non-repudiation, meeting the burgeoning need for handling colossal datasets with ever-decreasing latencies in computer networks. This technological surge coincides with remarkable advancements in artificial intelligence (AI) and machine learning (ML), which have emerged as pivotal facilitators in shaping the future of networks.

This special edition dedicates itself to exploring these transformative technologies that not only redefine the reliability of computer networks but also pave the way for novel distributed security services and applications. The papers encapsulated in this edition delve into various critical subjects, ranging from innovative cryptographic models applied in healthcare to intelligent threat detection systems and the introduction of novel consensus mechanisms within the blockchain domain.

Amid these contributions, six notable papers have undergone rigorous evaluation by experts, each presenting innovative solutions. Marcela Tuler de Oliveira et al. introduce the 'Break-Glass Protocol' employing Ciphertext-Policy Attribute-Based Encryption for secure medical record access during emergencies. Hélio do Nascimento Cunha Neto et al. propose 'MineCap,' a 'Super Incremental Learning' approach combating unauthorized cryptocurrency mining. Fabio Cesar Schuartz et al. focus on 'Improving Threat Detection in Networks Using Deep Learning,' and Vanessa Chicarino et al. tackle 'Detection of Selfish Mining and Stalker Attacks in Blockchain Networks.' Samuel Masseport et al. present 'Proof of Usage,' a user-centric consensus protocol, and Gabriel Reis Carrara et al. conduct a survey on 'Consistency, Availability, and Partition Tolerance in Blockchain: A Survey on Consensus Mechanisms over Peer-to-Peer Networking.'

In essence, these select papers epitomize cutting-edge research in distributed systems and network security. They offer a diverse spectrum of perspectives, insights, and innovative solutions that steer the course for fortified reliability and security within computer networks.

Review

Blockchain and artificial intelligence for network security

Mattos, D.M.F., Krief, F. & Rueda, S.J.

The featured research explores blockchain's impact on trustless applications and the evolution of next-gen networks empowered by AI and machine learning. This edition spotlights innovative advancements shaping reliable computer networks and distributed security services. Papers delve into diverse topics, like healthcare encryption, cryptocurrency mining detection, deep learning in threat detection, malicious behavior detection in blockchains, user-centric consensus, and blockchain consensus mechanisms. Authors propose novel protocols for secure data access during emergencies, sophisticated learning models for blocking unauthorized mining, and innovative consensus strategies. The survey assesses consensus mechanisms' costs and drawbacks in blockchain networks, charting new directions for enhanced reliability and security.

Blockchain Security Attacks, Challenges, and

Solutions for the Future Distributed

IoT Network

SAURABH SINGH,A. S. M. SANWAR HOSEN

AND BYUNGUN YOON

The research spotlights blockchain's central security feature—data secured within its transaction blocks. Governments globally integrate blockchain in numerous IoT applications, surveyed extensively in this study. The paper systematically dissects blockchain's attack surface, focusing on cryptographic constructs, architecture, and contextual applications, proposing detailed solutions. It dives into security issues, challenges, and solutions in blockchain and IoT integration. Analyses cover decentralization's pivotal role, consensus protocols, anonymity, user behavior, and regulatory compliance. Existing solutions explored encompass healthcare, financial sectors, vulnerabilities, and unanswered questions surrounding IoT and blockchain integration, emphasizing blockchain's transformative impact on the IT industry.

Systematic Review of Security Vulnerabilities in

Ethereum Blockchain Smart Contract

SATPAL SINGH KUSHWAHA SANDEEP JOSHI

DILBAG SINGH MANJIT KAUR

AND HEUNG-NO LEE

The papers extensively analyse vulnerabilities in Ethereum smart contracts, emphasizing the importance of comprehensive understanding among developers, students, and researchers. They categorize vulnerabilities into root causes and sub-causes, discuss real-life attacks, and propose detection tools and preventive measures to mitigate risks. Prevention methods encompass access control, careful function naming, gas optimization, and specific approaches to address diverse vulnerabilities like re-entrancy and integer overflow/underflow.

Several summaries emphasize the need for improved security tools, the challenges posed by Ethereum's scalability, and future research directions for enhancing vulnerability detection. Topics span gas mechanisms, DAOs, formal verification, privacy, and design patterns related to Ethereum blockchain technology and smart contracts.

In brief, these works serve as vital resources, offering in-depth insights into Ethereum smart contract vulnerabilities, preventive strategies, and the evolving landscape of blockchain security. They aim to provide comprehensive analyses and guidelines to fortify Ethereum smart contracts against potential threats.

An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network

Aitizaz Ali , Mohammed Amin Almaiah , Fahima Hajjej , Muhammad Fermi Pasha , Ong Huey Fang , Rahim Khan , Jason Teo , Muhammad Zakarya

This research explores blockchain's privacy issues in Industrial IoT (IIoT). It emphasizes the risks associated with transaction privacy in critical IIoT setups. Though searchable encryption (SE) mitigates these risks, current methods lack flexibility and anonymity. The paper proposes a blockchain-driven secure searchable encryption for multi-site clinical systems using homomorphic encryption on Hyperledger Fabric. Results use Hyperledger Calliper, evaluating encryption efficiency and network parameters across 3050 rounds. Privacy challenges in blockchain technologies, like Ethereum, highlight potential threats in IIoT landscapes due to their distributed ledger design. The study prompts a critical look at blockchain's privacy concerns in vital industries like IIoT.

A Novel Decentralized Blockchain Architecture for the Preservation of Privacy and Data Security against Cyberattacks in Healthcare

Ajitesh Kumar , Akhilesh Kumar Singh Ijaz Ahmad , Pradeep Kumar Singh , Anushree Pawan Kumar Verma , Khalid A Alissa Mohit Bajaj , Ateeq Ur Rehman 7 Elsayed Tag-Eldin

The research paper delves into blockchain's application in securing healthcare data. It emphasizes the healthcare sector's significance and outlines blockchain's decentralized nature, pivotal for data integrity. Previous studies exploring blockchain in various sectors, including healthcare, are discussed, citing prototypes like MedRec and underscoring scalability and security issues. The proposed approach introduces a secure healthcare data management system using a blockchain-based architecture, leveraging Bitcoin's decentralized model. Detailed descriptions are provided for processes like secure hashing encryption, block creation, proof of work, and implementation using Python's Flask framework. Performance analysis reveals the proposed architecture's efficiency in reducing data transmission compared to traditional Bitcoin and Lightweight networks, indicating a 63% reduction in total processing time. The conclusions emphasize the study's success in proposing a novel mechanism for secure healthcare data management, highlighting improved security, reduced traffic growth, transparency, traceability, and robustness. Details regarding data availability are offered upon request from the corresponding author.

On Blockchain-Based Cross-Service Communication and

Resource Orchestration on Edge Clouds

Konstantinos Papadakis-Vlachopapadopoulos , Ioannis Dimolitsas

, Dimitrios Dechouniotis

Eirini Eleni Tsiropoulou Ioanna Roussaki and Symeon Papavassiliou

This study explores the correlation between weather and chronic pain symptoms, addressing historical ambiguity. Past research suffered from small samples and study duration, limited weather conditions, and diverse designs. To gather substantial data, the study recruited 10,584 participants with complete baseline information. Out of 13,207 app downloads, 6850 individuals persisted past the first week, with 2658 involved in the final analysis. The research revealed higher humidity, increased wind speed, and lower atmospheric pressure amplifying pain severity in chronic pain patients. Relative humidity notably impacted pain levels, suggesting specific weather conditions elevate pain occurrence by over 20% compared to average days. Patient engagement played a crucial role in this study's success.

EDISON: A Blockchain-based Secure and

Auditable Orchestration Framework for

Multi-domain Software Defined Networks

Chandrasekar Balachandran, Puneet A.C, Gowri Ramachandran, and Bhaskar Krishnamachari

The introduction highlights Software-Defined Networks (SDN) and zero-trust security principles used in emerging 5G/6G technologies, separating control and data planes for heightened security. Addressing gaps in existing systems, the proposed solution focuses on decentralized authentication in multi-tenant SDNs.

Current networking standards, including SDN and multi-tenant environments, demand decentralized authentication, robust SLA monitoring, and transparent, decentralized logging. Previous studies presented blockchain-based approaches but lacked comprehensive SLA adherence and authentication protocols.

The motivation emphasizes the need for a novel Public Key Infrastructure (PKI) and Kerberos authentication to counter blind trust issues in SD-WANs, especially in multi-stakeholder environments.

The EDISON framework integrates blockchain, smart contracts, and decentralized applications to create a secure, auditable, and decentralized orchestration system. Its operational flow describes the authentication and logging process, enabling automated orchestration in complex networking environments.

Security and trust analysis reveal EDISON's ability to mitigate vulnerabilities and ensure transparent, secure logging, offering micro-segmentation for enhanced security. Implementation evaluation demonstrates minor delays in EDISON's authentication process, but blockchain throughput varies based on the chosen platform.

The conclusion highlights EDISON's role in providing robust authentication, auditing, and orchestration in SD-WANs, offering flexible, secure, and efficient solutions to security vulnerabilities.

Blockchain and artificial intelligence for network security

Diogo Menezes Ferrazani Mattos & Francine Krief & Sandra Julieta Rueda

Blockchain represents an innovative technology facilitating the creation of trustworthy applications without necessitating trust among network participants. Concurrently, artificial intelligence (AI) and machine learning (ML) methods have seen remarkable advancements, becoming pivotal elements for forthcoming networks. This special edition focuses on these transformative technologies, aiming to fortify computer networks while facilitating novel security applications and services based on distributed and knowledge-driven approaches.

The included papers explore diverse themes, such as innovative cryptographic models for healthcare, intelligent threat detection systems, and fresh consensus mechanisms for blockchains. For instance, authors propose an attribute-based encryption system to enable access to encrypted Electronic Medical Records (EMRs) during critical stroke treatments. Other contributions delve into combating unauthorized cryptocurrency mining in corporate networks, enhancing threat detection using deep learning methods, identifying malicious activities within blockchain networks, introducing user-centric consensus protocols, and conducting comprehensive surveys on blockchain consensus mechanisms, evaluating their drawbacks and associated costs.

Cyber Security through Blockchain Technology

Alex. R. Mathew

Blockchain, a revolutionary technology, guarantees immutable, open, and distributed data. Any block alteration changes its hash, affecting subsequent blocks, ensuring immutability. This study analyzes 30 research papers on Blockchain cybersecurity. Results highlight IoT, network, and data storage as prominent focuses due to weak security configurations and increased data theft. Blockchain secures IoT through robust authentication, preventing device breaches. It fortifies networks, obstructing unauthorized access. Future research should explore a unified Blockchain for seamless security solutions, as current variations hinder integration. Blockchain technology, continuously evolving, offers promising solutions for cybersecurity challenges in IoT, networks, and data storage.

Discussion

The integration of blockchain technology within healthcare systems has garnered substantial attention due to its potential in fortifying data security and integrity. Various research studies spotlight its pivotal role in enhancing security across Electronic Medical Records (EMRs), Electronic Health Records (EHRs), patient monitoring, and pharmaceutical supply chains. Through innovative methodologies like blockchain-based access control and secure encryption, these studies emphasize the importance of safeguarding sensitive medical records against tampering and unauthorized access.

The collective findings of these research endeavours underscore the advantages and limitations of incorporating blockchain in healthcare. Notably, blockchain presents significant advantages in enhancing data security, transparency, traceability, and overall robustness in managing healthcare data. However, inherent challenges, including scalability issues and resource-intensive operations, pose notable obstacles to widespread implementation.

Comparative analyses against traditional networks, including Bitcoin and Lightweight networks, highlight the efficiency and potential of novel blockchain architectures. These studies demonstrate noteworthy reductions in total processing time and advancements in data security, showcasing the unique contributions made within the realm of healthcare data management.

Moving beyond healthcare, the discussion extends to blockchain's pivotal role in fortifying network security, especially concerning IoT devices, network infrastructure, and data storage. In the landscape of IoT security, blockchain's decentralized architecture presents a formidable solution to enhance security protocols. Its immutable and decentralized nature provides reliable authentication mechanisms and ensures data integrity, thus significantly reducing the risk of breaches within IoT devices.

Furthermore, blockchain exhibits promise in fortifying the integrity and resilience of network infrastructure. Its stringent infrastructure effectively thwarts unauthorized access attempts, fostering secure communication environments within networks. However, the challenge of integrating diverse blockchain variations inhibits seamless deployment across network environments, indicating a need for further research focusing on unifying blockchain systems.

In the domain of data storage, blockchain emerges as a critical component in ensuring data integrity and combatting data breaches. With its immutable ledger and cryptographic features, blockchain offers robust mechanisms for safeguarding sensitive data. Its application in data storage security presents substantial potential to prevent unauthorized access, thereby providing a more resilient shield against data breaches.

While acknowledging blockchain's pivotal role in bolstering healthcare and network security, addressing existing challenges, such as scalability and integration complexities, remains imperative. Future research endeavors should concentrate on developing unified blockchain architectures to streamline security solutions, promoting interoperability among different systems for comprehensive network security.

In conclusion, blockchain technology stands as a beacon of hope in ameliorating cybersecurity vulnerabilities across healthcare and network domains. Its deployment promises fortified authentication mechanisms, enhanced data integrity, and robust network defense mechanisms. Nonetheless, overcoming integration challenges by unifying blockchain platforms is crucial to harness its full potential in fortifying contemporary security paradigms.

Conclusion

Blockchain technology has exhibited significant evolution and broad applicability across various domains, especially in addressing security challenges in IoT, networks, and data transmission. The technology's potential to enhance authentication and data integrity in IoT devices is vital for thwarting potential breaches arising from poor security setups. Additionally, blockchain's stringent infrastructure fortifies networks by preventing unauthorized access and communication, particularly in critical environments like IIoT.

Blockchain technology continues to evolve and find more use cases in the modern world.

The Blockchain infrastructure makes it highly practical in addressing the existing security challenges in areas such as IoT devices, networks, and data in transmission and storage.

Other major areas of Blockchain security are networks and data.

As observed in the discussion, the Blockchain technology can be used to secure IoT devices through more reliable authentication and data transfer mechanisms.

These can prevent hackers from breaching into these devices which often ship with poor security configurations.

The technology can be used to secure networks by using the stringent infrastructure to prevent unauthorized connections and communication[15].

It is recommended that future researchers look into the practicality of a single Blockchain that can be used to develop security solutions since most of the current solutions use different Blockchains hampering integration conclusion

Blockchain has been one of the most hyped technologies in the past 5 years due to its popularity gained by its various cryptocurrencies.

While blockchains including Ethereum provide important anonymity, integrity, and auditability features for its users, there are important privacy and security risks that were discussed and presented in this paper related to their use in critical environments, such as IIoT environments.

These privacy issues exist in other blockchains as one of their main design principles utilizes distribution of ledger.

We implemented the novel comprehensive approach of homomorphic encryption in the digital healthcare system using blockchain technology that provides a secure keyword search facility at the user’s end.