

Chapter 3

Artificial Intelligence, Blockchain Framework, Cyberthreat Defenses of Resilient Digital Ecosystems

Heru Susanto

 <https://orcid.org/0000-0002-1823-357X>

Center for Research Collaboration of Graph Theory and Combinatory, Center for Innovative Engineering, School of Business, Universiti Teknologi Brunei, Brunei & Center for Data Sciences, Data and Information Security Group, National Research and Innovation Agency, Indonesia

Mohammad Qawiul Azim

Center for Innovative Engineering, School of Business, Universiti Teknologi Brunei, Brunei

Leu Fang-Yie

Center for Research Collaboration of Graph Theory and Combinatory, Department of Computer Science, Tunghai University, Taiwan

Alifya Kayla Shafa Susanto`

Center for Research Collaboration of Graph Theory and Combinatory, Department of Information Security, School of Computing and Informatics, Universiti Teknologi Brunei, Brunei

Desi Setiana

Ministry of Law and Human Right, Indonesia & Universiti Brunei Darussalam, Brunei

Fahmi Ibrahim

 <https://orcid.org/0000-0001-5016-7755>

School of Business, Universiti Teknologi Brunei, Brunei

Akbari Indra Basuki

Center for Data Sciences, Data and Information Security Group, National Research and Innovation Agency, Indonesia

Taufik Iqbal Ramdhani

 <https://orcid.org/0000-0001-7436-4884>

Center for Data Sciences, Data and Information Security Group, National Research and Innovation Agency, Indonesia

Iwan Setiawan

Center for Data Sciences, Data and Information Security Group, National Research and Innovation Agency, Indonesia & Center for Research Collaboration of Graph Theory and Combinatory, Universitas Indonesia, Indonesia


Budhi Riyanto

Center for Data Sciences, Data and Information Security Group, National Research and Innovation Agency, Indonesia

Rd Angga Ferianda

Center for Data Sciences, Data and Information Security Group, National Research and Innovation Agency, Indonesia

Arief Indriarto Haris

 <https://orcid.org/0000-0002-5163-3540>

Center for Data Sciences, Data and Information Security Group, National Research and Innovation Agency, Indonesia

Raden Muhammad Taufik Yuniantoro

Center for Data Sciences, Data and Information Security Group, National Research and Innovation AgencyTeknologi, Indonesia

Ulaganathan Subramanian

School of Business, Universiti Teknologi Brunei, Brunei

DOI: 10.4018/978-1-6684-5849-5.ch003

ABSTRACT

A rise in the number of digital ecosystem users, as well as an increase in cyberthreats, has occurred in recent years. Risk of security breaches puts important data at risk for the public. With its high-level encryption security features, blockchain technology keeps data safe from unauthorized access. The study's goal is to find out if the blockchain framework can withstand the modern cyberthreats that exist inside the digital ecosystem today. It is critical that consumers are informed of the potential dangers of their online activities. These cyberthreats have been identified in the digital environment according to the research. An additional focus of the research is on identifying and resolving any security vulnerabilities with blockchain technology. The problem statement of the study, which is cyberthreat, is discussed in the introduction. It is also important to understand how blockchain operates and evaluate its security. Aim and purpose of the research are outlined in the introduction. The literature review discusses the study identified areas, gaps toward the issue, and the strategy to dealing with the gaps. The study's research approach makes use of a survey questionnaire and a random sample method to conduct descriptive research. Approximately 100 people are expected to participate in the survey. The analysis will be based on the figure itself where we evaluate based on how it shows. As a consequence, this finishes the study and provides further recommendations.

INTRODUCTION

Background of the Study

Cyberthreats are more likely to occur due to the rising use of digital technologies. Cyberthreats include anything from data theft and tampering to data erasure and other criminal activities. Individuals are concerned about the safety of their personal data in the digital economy because of this. Blockchain technology, on the other hand, may be utilized as a preventative measure against this problem. It is possible to run a safe computing environment in an open system without the requirement for a central authority using the blockchain. Blockchain is being used by a number of companies to boost productivity and provide a return on their investment. In order to reduce operating expenses, it is widely accepted that blockchain has the ability to do operations more efficiently. An increasing number of businesses are using blockchain technology to safeguard and track their work processes across systems borders.

Cyber security has become a serious issue in the digital sector, as data is no longer protected from being hacked. The number of internet users is likely to climb in the next years due to the growing number of people using the internet. Increased user numbers necessitate additional data management and security measures. Cybercrime is estimated to damage the global economy an estimated trillions every year. The frequency and complexity of cyberattacks are on the rise, making the situation even worse (Chiu et al., 2022; Susanto, 2021). For the digital sector, Blockchain is now considered the most secure method of storing and transmitting data. Its capabilities reveal that it has features such as data secrecy, integrity, and availability that are superior to those of currently available technologies. When it comes to data security and commercial transactions, it is regarded a viable technology.

A blockchain is a chronological series of documents called blocks that stores data openly. Users' privacy is protected by employing cryptography to encrypt information so that it cannot be read or changed. A blockchain network does not have a centralized control, unlike existing financial organizations. Each blockchain transaction is democratically approved by the network's members, who are in

26 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/artificial-intelligence-blockchain-framework-cyberthreat-defenses-of-resilient-digital-ecosystems/314438

Related Content

A Multimodal Sentiment Analysis Model for Graphic Texts Based on Deep Feature Interaction Networks

Wanjun Chang and Dongfang Zhang (2024). *International Journal of Ambient Computing and Intelligence* (pp. 1-19).

www.irma-international.org/article/a-multimodal-sentiment-analysis-model-for-graphic-texts-based-on-deep-feature-interaction-networks/355192

Blockchain for Healthcare: Safe Data Sharing in the AIoMT Era

Madiha Munawar, Thakur Monika Singh, C. Kishor Kumar Reddy and Srinath Doss (2025). *Utilizing AI of Medical Things for Healthcare Security and Sustainability* (pp. 369-400).

www.irma-international.org/chapter/blockchain-for-healthcare/375198

Green Software Development: Integrating AI for Energy Efficiency

C. V. Suresh Babu, Shifa Sherin M. and S. Rufus (2025). *Sustainable Information Security in the Age of AI and Green Computing* (pp. 157-174).

www.irma-international.org/chapter/green-software-development/380042

The Virtual Twin: A Socialization Agent for Peer-to-Peer Networks

Alexandre Gachet and Pius Haettenschwiler (2005). *International Journal of Intelligent Information Technologies* (pp. 56-67).

www.irma-international.org/article/virtual-twin-socialization-agent-peer/2384

Security Framework for Smart Visual Sensor Networks

G. Suseela and Y. Asnath Vicky Phamila (2021). *Research Anthology on Artificial Intelligence Applications in Security* (pp. 250-268).

www.irma-international.org/chapter/security-framework-for-smart-visual-sensor-networks/270601