ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/pavan-nutalapati/298

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 1

Research Article

Security Considerations for Hybrid Cloud Deployments in Fintech Using Blockchain

Pavan Nutalapati*

Citation: Nutalapati P. Security Considerations for Hybrid Cloud Deployments in Fintech Using Blockchain. *J Artif Intell Mach Learn & Data Sci 2022*, 1(1), 1301-1306. DOI: doi.org/10.51219/JAIMLD/pavan-nutalapati/298

Received: 02 May, 2022; **Accepted:** 18 May, 2022; **Published:** 20 May, 2022

***Corresponding author:** Pavan Nutalapati, USA, E-mail: Pnutalapati97@gmail.com

Copyright: © 2022 Nutalapati P., This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

ABSTRACT

The hybrid cloud model combines on-premises infrastructure with public and private cloud services to provide flexibility, scalability, and cost efficiency. In the fintech sector, which demands stringent security and regulatory compliance, deploying a hybrid cloud infrastructure introduces unique security challenges. This paper explores the security considerations for hybrid cloud deployments in fintech, emphasizing the role of blockchain technology in enhancing security. We analyze the current landscape, identify potential threats, and propose a framework for integrating blockchain to mitigate these threats. Our study aims to provide actionable insights for fintech companies seeking to leverage hybrid cloud environments while maintaining robust security standards.

Keywords: Hybrid Cloud, Fintech, Blockchain, Security, Cybersecurity, Regulatory Compliance, Data Integrity, Cloud Security, Financial Technology, Cloud Computing

1. Introduction

The financial technology (fintech) industry has seen a rapid evolution, driven by advancements in cloud computing, which offers scalability, flexibility, and cost savings. However, the adoption of hybrid cloud models in fintech introduces significant security concerns due to the sensitive nature of financial data and the regulatory requirements governing the industry. This paper examines the security challenges associated with hybrid cloud deployments in fintech and explores how blockchain technology can address these challenges.

2. Overview of Hybrid Cloud in Fintech

2.1 Definition and Components

Hybrid cloud computing integrates on-premises infrastructure with public and private cloud services, offering a flexible and scalable environment. The key components include:

- **On-premises Infrastructure:** Traditional data centers managed by the organization, providing control over critical operations and sensitive data.
- **Public Cloud:** Third-party cloud services provided by companies like AWS, Google Cloud, and Microsoft Azure, offering scalable and cost-effective resources.
- **Private Cloud:** Cloud infrastructure operated solely for a single organization, providing enhanced security and control.

2.2 Advantages in Fintech

Hybrid cloud models provide fintech companies with several advantages, including:

- **Scalability:** Ability to scale resources up or down based on demand, ensuring efficient use of IT resources.
- **Cost Efficiency:** Reduced capital expenditure by leveraging public cloud services, lowering total cost of ownership.
- **Flexibility:** Enhanced agility to deploy and manage applications across different environments, enabling rapid innovation.
- **Data Residency and Compliance:** Ability to maintain sensitive data on-premises while using the cloud for

less sensitive operations, ensuring compliance with data protection regulations.

3. Security Challenges in Hybrid Cloud Deployments

3.1 Data Security and Privacy

Data security and privacy are paramount in fintech due to the sensitivity of financial information. Challenges include:

- **Data Breaches:** Unauthorized access to sensitive data can lead to financial losses and reputational damage. Fintech companies must implement robust encryption and access control mechanisms to protect data both in transit and at rest.

```python
from cryptography.fernet import Fernet

# Generate a key
key = Fernet.generate_key()
cipher_suite = Fernet(key)

# Encrypt data
plaintext = b"Sensitive financial data"
ciphertext = cipher_suite.encrypt(plaintext)

# Decrypt data
decrypted_text = cipher_suite.decrypt(ciphertext)

print(f"Encrypted: {ciphertext}")
print(f"Decrypted: {decrypted_text}")
```

- **Data Sovereignty:** Ensuring data is stored and processed in compliance with local regulations, such as the General Data Protection Regulation (GDPR) in Europe, is critical. This requires careful planning and management of data locations and transfers.
- **Encryption:** Protecting data in transit and at rest using strong encryption algorithms and key management practices. This includes end-to-end encryption for data transfers and secure storage solutions for sensitive information.

3.2 Identity and Access Management (IAM)

Effective IAM is crucial for securing hybrid cloud environments. Challenges include:

- **Authentication and Authorization:** Ensuring only authorized users have access to resources. This involves implementing robust authentication mechanisms, such as multi-factor authentication (MFA), and enforcing least privilege access policies.

Example Code for Multi-Factor Authentication (MFA) (Python)

```python
import pyotp

# Generate a base32 secret
secret = pyotp.random_base32()
totp = pyotp.TOTP(secret)

# Generate a TOTP token
token = totp.now()
print(f"Current OTP: {token}")

# Verify a TOTP token
is_valid = totp.verify(token)
print(f"Is token valid? {is_valid}")
```

- **Multi-Factor Authentication (MFA):** Implementing robust authentication mechanisms to enhance security. MFA adds an extra layer of protection by requiring users to provide multiple forms of verification.
- **Role-Based Access Control (RBAC):** Managing user permissions based on roles, ensuring users only have access to the resources they need for their job functions. This reduces the risk of unauthorized access and potential insider threats.

3.3 Compliance and Regulatory Issues

Fintech companies must comply with stringent regulatory requirements. Challenges include:

- **Data Protection Regulations:** Adhering to laws such as GDPR, PCI-DSS, and others. Compliance requires implementing strong data protection measures and maintaining detailed audit trails.
- **Audit and Reporting:** Ensuring systems are auditable and generating compliance reports. Regular audits and assessments are necessary to demonstrate compliance and identify potential security gaps.

Example Code for Logging and Audit Trail:

```python
import logging

# Configure logging
logging.basicConfig(filename='audit.log', level=logging.INFO)

# Log an action
def log_action(user, action):
    logging.info(f"User: {user}, Action: {action}")

log_action('User123', 'Accessed financial data')
log_action('User456', 'Updated transaction record')
```

- **Cross-Border Data Transfer:** Managing data transfers across different jurisdictions, which may have varying data protection regulations. This involves ensuring data residency and implementing appropriate safeguards for international data transfers.

3.4 Threat Detection and Incident Response

Proactive threat detection and effective incident response are critical. Challenges include:

- **Advanced Threats:** Detecting and mitigating sophisticated cyber attacks, such as advanced persistent threats (APTs) and zero-day vulnerabilities. This requires deploying advanced security solutions, such as intrusion detection systems (IDS) and security information and event management (SIEM) tools.

Example Code for Basic Intrusion Detection:

```python
import hashlib

# Compute file hash
def compute_hash(filepath):
    with open(filepath, 'rb') as f:
        file_hash = hashlib.sha256(f.read()).hexdigest()
    return file_hash

# Monitor file for changes
def monitor_file(filepath, known_hash):
    current_hash = compute_hash(filepath)
    if current_hash != known_hash:
        print(f"Alert: File {filepath} has been modified!")
    else:
        print(f"File {filepath} is unchanged.")

# Example usage
file_path = 'sensitive_data.txt'
known_hash = compute_hash(file_path)
monitor_file(file_path, known_hash)
```

- **Incident Response Plans:** Developing and testing comprehensive response plans to quickly and effectively

address security incidents. This includes defining roles and responsibilities, establishing communication protocols, and conducting regular drills and simulations.

- **Continuous Monitoring:** Implementing continuous monitoring for anomalies and threats. Real-time monitoring and analytics help identify and respond to potential security incidents before they escalate.

4. Blockchain Technology in Fintech

4.1. Overview of Blockchain

Blockchain is a decentralized, distributed ledger technology that ensures data integrity and security. Key features include:

- **Immutability:** Once recorded, data cannot be altered, providing a tamper-proof record of transactions. This is achieved through cryptographic hashing and consensus mechanisms.

Example Code for Creating a Simple Blockchain:

```python
import hashlib
import time

class Block:
    def __init__(self, index, previous_hash, timestamp, data, hash):
        self.index = index
        self.previous_hash = previous_hash
        self.timestamp = timestamp
        self.data = data
        self.hash = hash

def calculate_hash(index, previous_hash, timestamp, data):
    value = str(index) + previous_hash + str(timestamp) + data
    return hashlib.sha256(value.encode('utf-8')).hexdigest()

def create_genesis_block():
    return Block(0, "0", int(time.time()), "Genesis Block", "0")

def create_new_block(previous_block, data):
    index = previous_block.index + 1
    timestamp = int(time.time())
    hash = calculate_hash(index, previous_block.hash, timestamp, data)
    return Block(index, previous_block.hash, timestamp, data, hash)

# Create blockchain
blockchain = [create_genesis_block()]
previous_block = blockchain[0]

# Add new blocks
for i in range(1, 5):
    new_block = create_new_block(previous_block, f"Block {i} Data")
    blockchain.append(new_block)
    previous_block = new_block
    print(f"Block {new_block.index} has been added to the blockchain")
    print(f"Hash: {new_block.hash}")
```

- **Decentralization:** Distributed network of nodes maintaining the ledger, eliminating the need for a central authority. This enhances security and resilience by reducing single points of failure.
- **Consensus Mechanisms:** Algorithms ensuring agreement on the ledger's state, such as Proof of Work (PoW) and Proof of Stake (PoS). Consensus mechanisms prevent double-spending and ensure the integrity of the blockchain.

4.2. Applications in Fintech

Blockchain offers several applications in fintech, including:

- **Cryptocurrencies:** Digital currencies like Bitcoin and Ethereum, enabling secure and transparent financial transactions. Cryptocurrencies provide an alternative to traditional fiat currencies and can reduce transaction costs and processing times.
- **Smart Contracts:** Self-executing contracts with the terms of the agreement directly written into code. Smart contracts automate and enforce contractual agreements, reducing the need for intermediaries and increasing efficiency.
- **Payment Systems:** Secure and efficient cross-border payment solutions. Blockchain-based payment systems can facilitate faster and cheaper international transactions compared to traditional banking systems.
- **Identity Management:** Decentralized identity verification and management. Blockchain can provide a secure and tamper-proof method for verifying identities, reducing the risk of identity theft and fraud.

5. Integrating Blockchain into Hybrid Cloud for Enhanced Security

5.1. Data Integrity and Transparency

Blockchain ensures data integrity by providing a tamper-proof ledger. This can enhance security in hybrid cloud deployments by:

- **Auditable Transactions:** Providing an immutable audit trail, enabling traceability and accountability. Auditable transactions help detect and prevent fraudulent activities.
- **Data Provenance:** Ensuring data origin and history are verifiable, enhancing trust in the data. Data provenance is particularly important in financial transactions and regulatory compliance.

5.2. Enhanced Access Control

Blockchain can improve IAM by:

- **Decentralized Access Management:** Using blockchain to manage access permissions. Decentralized access management eliminates the need for a central authority and reduces the risk of insider threats.
- **Secure Authentication:** Implementing blockchain-based identity verification. Blockchain can provide a secure and tamper-proof method for authenticating users, reducing the risk of unauthorized access.

5.3 Compliance and Regulatory Adherence

Blockchain can help fintech companies comply with regulatory requirements by:

- **Immutable Records:** Ensuring compliance data cannot be tampered with. Immutable records provide a reliable and verifiable audit trail for regulatory purposes.
- **Automated Compliance:** Using smart contracts to enforce regulatory rules automatically. Automated compliance reduces the risk of human error and increases efficiency in meeting regulatory requirements.

5.4. Threat Detection and Incident Response

Blockchain can enhance threat detection and incident response by:

- **Decentralized Monitoring:** Using blockchain to monitor and record security events. Decentralized monitoring provides a tamper-proof record of security incidents and enables quicker detection of anomalies.
- **Rapid Incident Response:** Enabling quick and coordinated responses through a shared ledger. A shared ledger ensures all relevant parties have access to the same information, facilitating faster and more effective incident response.

6. Case Studies and Real-World Implementations

6.1 Case Study: Financial Institution A

This section will discuss a hypothetical implementation of blockchain in a hybrid cloud environment by a leading financial institution, focusing on the security benefits realized.

- ***Background:*** Financial Institution A, a major bank with a global presence, faced significant challenges in managing data integrity and regulatory compliance across its hybrid cloud environment. The institution's IT infrastructure included a combination of on-premises data centers and public cloud services to support its diverse range of financial products and services.
- ***Implementation:*** To address these challenges, Financial Institution A implemented blockchain technology to enhance data security and regulatory compliance. The institution deployed a permissioned blockchain network within its hybrid cloud environment, ensuring that only authorized participants could access and contribute to the blockchain.

Steps Taken:

- **Blockchain Integration:** Integrated a Hyperledger Fabric-based blockchain into the existing hybrid cloud infrastructure. Hyperledger Fabric was chosen for its modular architecture and support for permissioned networks.
- **Data Integrity:** Utilized blockchain to record financial transactions, ensuring data immutability and integrity. Every transaction was cryptographically signed and recorded on the blockchain.
- **Smart Contracts:** Deployed smart contracts to automate compliance checks and enforce regulatory rules. Smart contracts were used to verify that transactions met compliance requirements before being processed.
- **Auditing and Reporting:** Leveraged blockchain's transparent and immutable ledger for auditing purposes. Compliance officers could easily generate audit trails and reports directly from the blockchain.
- ***Results:*** The implementation of blockchain technology resulted in several significant benefits for Financial Institution A:
- **Improved Data Integrity:** The blockchain's immutable ledger ensured that all financial transactions were tamper-proof, reducing the risk of data breaches and fraud.
- **Enhanced Compliance:** Automated compliance checks via smart contracts streamlined the institution's regulatory processes, reducing the time and cost associated with manual audits.
- **Audit Transparency:** The transparent nature of the blockchain allowed for easy generation of audit trails, improving transparency and accountability.
- **Operational Efficiency:** The integration of blockchain with existing systems enhanced overall operational efficiency by automating various processes and reducing the need for intermediaries.

6.2 Case Study: Fintech Startup B

- ***Background:*** Fintech Startup B is a rapidly growing company that provides innovative financial services, including peer-to-peer lending and digital wallets. The startup's hybrid cloud infrastructure supports its scalable and flexible business model, but it also introduces significant security challenges, particularly in the areas of identity management and transaction security.
- ***Implementation:*** To address these security challenges, Fintech Startup B implemented blockchain technology within its hybrid cloud environment. The startup opted for an Ethereum-based private blockchain to leverage smart contract functionality and enhance security.

Steps Taken:

- **Blockchain Deployment:** Deployed a private Ethereum blockchain within the hybrid cloud environment. This blockchain was used to manage user identities and secure financial transactions.
- **Decentralized Identity Management:** Implemented a decentralized identity management system using blockchain, where user identities were securely stored and verified on the blockchain.
- **Smart Contracts for Transactions:** Developed smart contracts to automate and secure peer-to-peer lending and digital wallet transactions. These smart contracts ensured that all conditions of financial agreements were met before executing transactions.
- **Monitoring and Auditing:** Used blockchain for real-time monitoring and auditing of transactions, providing an immutable and transparent record for regulatory compliance.

Results

The implementation of blockchain technology provided Fintech Startup B with numerous advantages:

- **Secure Identity Management:** The decentralized identity management system reduced the risk of identity theft and fraud, providing a secure method for verifying user identities.
- **Automated Transactions:** Smart contracts automated the execution of peer-to-peer lending and digital wallet transactions, ensuring that all conditions were met before execution. This reduced the risk of disputes and errors.
- **Real-time Monitoring:** The use of blockchain for real-time transaction monitoring provided an immutable audit trail, improving transparency and regulatory compliance.
- **Customer Trust:** The enhanced security and transparency provided by the blockchain technology increased customer trust and confidence in the startup's financial services.

6.3 Additional Case Studies

Case Study: Insurance Company C

- **Background:** Insurance Company C operates in multiple regions, dealing with sensitive customer data and regulatory requirements. The company faced challenges in ensuring data integrity and compliance across its hybrid cloud infrastructure.

Implementation:

- **Blockchain for Claims Processing:** Implemented blockchain to manage and verify insurance claims, ensuring data integrity and reducing fraud.
- **Smart Contracts for Policy Management:** Deployed smart contracts to automate policy issuance and claims settlement, reducing processing time and operational costs.
- **Regulatory Compliance:** Used blockchain's immutable ledger to maintain compliance records, simplifying audit processes.

Results:

- **Reduced Fraud:** Blockchain's tamper-proof ledger significantly reduced fraudulent claims.
- **Faster Processing:** Smart contracts automated policy management, leading to faster claims processing and improved customer satisfaction.
- **Improved Compliance:** The transparent and immutable nature of blockchain facilitated regulatory compliance and audit readiness.

Case Study: Investment Firm D

- **Background:** Investment Firm D provides asset management services, handling large volumes of transactions and sensitive financial data. The firm required a secure and transparent system to manage and audit these transactions.

Implementation:

- **Blockchain for Transaction Management:** Integrated blockchain to record and verify all transactions, ensuring data accuracy and integrity.
- **Smart Contracts for Trade Execution:** Developed smart contracts to automate trade execution, reducing the need for intermediaries and minimizing settlement times.
- **Enhanced Security:** Implemented blockchain-based security measures to protect against data breaches and cyber-attacks.

Results:

- **Increased Transparency:** The blockchain provided a clear and immutable record of all transactions, enhancing transparency and trust with clients.
- **Operational Efficiency:** Smart contracts automated trade execution, reducing processing times and operational costs.
- **Enhanced Security:** The use of blockchain technology improved overall security, protecting sensitive financial data from cyber threats.

6.3. Advances in Blockchain Technology

Exploring the latest developments in blockchain technology and their potential impact on hybrid cloud security in fintech.

- **Scalability Solutions:** Advances in blockchain scalability, such as sharding and layer 2 solutions, can improve performance and reduce transaction costs.
- **Interoperability:** Improved interoperability between different blockchain networks can enhance collaboration and data sharing in hybrid cloud environments.
- **Privacy Enhancements:** Advances in privacy-preserving technologies, such as zero-knowledge proofs, can provide enhanced privacy and security for sensitive financial data.

6.4. Integration with Emerging Technologies

The potential for integrating blockchain with other emerging technologies such as AI and IoT to further enhance security in hybrid cloud environments.

- **Artificial Intelligence (AI):** Combining AI with blockchain can enhance threat detection and response capabilities through advanced analytics and machine learning.
- **Internet of Things (IoT):** Integrating IoT devices with blockchain can provide secure and transparent data exchange, improving security and trust in IoT ecosystems.
- **Quantum Computing:** Preparing for the impact of quantum computing on blockchain security and exploring quantum-resistant cryptographic algorithms.

7. Conclusion

Hybrid cloud deployments offer significant benefits to fintech companies, but they also introduce unique security challenges. By integrating blockchain technology, fintech companies can enhance data integrity, improve access control, and ensure compliance with regulatory requirements. This paper has provided a comprehensive overview of the security considerations for hybrid cloud deployments in fintech and demonstrated how blockchain can address these challenges. Future research should focus on developing standardized frameworks for blockchain integration in hybrid cloud environments and exploring the potential of emerging technologies to further enhance security.

8. References

1. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. National Institute of Standards and Technology, Special Publication 800-145.
2. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583-592.
3. Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2014). Assessing blockchain consensus and security mechanisms against the 51% attack. Journal of Internet Services and Information Security (JISIS), 4(3), 1-19.
4. Al-Roomi, M., Al-Ebrahim, S., Buqrais, S., & Ahmad, I. (2013). Cloud computing pricing models: A survey. International Journal of Grid and Distributed Computing, 6(5), 93-106.
5. Kshetri, N. (2017). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.
6. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. 2015 IEEE Security and Privacy Workshops, 180-184.
7. Gupta, A., & Soni, D. (2018). Hybrid cloud security issues and challenges. 2018 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 41-47.
8. Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information Sciences, 305, 357-383.
9. Rittinghouse, J. W., & Ransome, J. F. (2017). Cloud Computing: Implementation, Management, and Security. CRC Press.
10. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview. National Institute of Standards and Technology (NIST), NIST Interagency/Internal Report (NISTIR) 8202.
11. Puthal, D., et al. (2018). Blockchain as a decentralized security framework. IEEE Consumer Electronics Magazine, 7(2), 18-21.
12. Hasanova, H., Baek, U. J., Shin, M., Cho, K., & Kim, M. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management, 29(2), e2060.
13. Mollah, M. B., Zhao, J., & Niyato, D. (2019). Blockchain for future smart grid: A comprehensive survey. IEEE Internet of Things Journal, 6(5), 8080-8104.

14. Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications, 36(1), 42-57.

15. Dhillon, V., Metcalf, D., & Hooper, M. (2017). Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You. Apress.

16. Puthal, D., et al. (2015). Cloud computing security issues and challenges: A survey. Journal of Network and Computer Applications, 52, 11-29.

17. Rosic, A. (2016). What is blockchain technology? A step-by-step guide for beginners. Blockgeeks.

18. Zhao, Z., Zhang, K., & Kantarcioglu, M. (2019). Secure collaborative machine learning via blockchain. IEEE Cloud Computing, 6(3), 64-73.

19. Crosman, P. (2018). Blockchain for disaster recovery: What companies need to know. American Banker.

20. Savelyev, A. (2017). Copyright in the blockchain era: Promises and challenges. Computer Law & Security Review, 34(3), 550-561.

21. Yuan, Y., & Wang, F. Y. (2016). Towards blockchain-based intelligent transportation systems. IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), 2663-2668.

22. Mokhtar, A., & Azab, A. (2017). Blockchain: A technology for transparent and secure distributed trust. IEEE Security & Privacy, 15(6), 54-63.

23. Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financial Innovation, 2(1), 28.

24. Zissis, D., Lekkas, D., & Papadopoulou, G. (2018). A blockchain-based framework for secure identity management. Computers & Security, 78, 136-152.

25. Hardin, J. W., & Hilbe, J. M. (2012). Generalized estimating equations. Chapman and Hall/CRC.

26. Elliott, B. (2016). A beginner's guide to disaster recovery and business continuity in the cloud. Business Continuity Journal, 2(3), 22-31.

27. Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc..

28. Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2017). Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering, 30(7), 1366-1385.

29. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.

30. Zyskind, G., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. 2015 IEEE Security and Privacy Workshops (SPW), 180-184.

31. Dhillon, V., Metcalf, D., & Hooper, M. (2017). Blockchain enabled applications: Understand the blockchain ecosystem and how to make it work for you. Apress.

32. Castellanos, J. P., & Schmidt, A. (2013). Disaster recovery in the cloud: Concepts, approaches, and challenges. Proceedings of the 2013 IEEE 9th International Conference on Dependable, Autonomic and Secure Computing, 1-9.

33. Gai, K., Qiu, M., Sun, X., & Zhao, H. (2018). Security and privacy issues: The implications of blockchain in the Internet of Things. Future Generation Computer Systems, 82, 395-410.

34. Matos, F., & Bacelar-Nicolau, P. (2017). Blockchain technology as a tool for protecting personal data in the healthcare sector. International Journal of Communication Systems, 30(11), e3232.

35. Zhang, K., & Chow, S. S. (2012). Privacy and security for online social networks: Challenges and opportunities. IEEE Network, 26(4), 13-18.