Towards Secure Blockchain-enabled Cloud Computing: A Taxonomy of Security Issues and Recent Advances

Shengli LIU*
Department of Public Basic Education, Hebi Polytechnic
Henan Hebi, 458030, China

***Abstract*—Blockchain technology offers a promising solution for addressing performance and security challenges within distributed systems. This paper presents a comprehensive taxonomy of security issues in cloud computing and explores recent advances in utilizing blockchain to enhance security and efficiency in this domain. We employ a systematic literature review approach to analyze various blockchain-enabled solutions for cloud computing. Our findings reveal that blockchain's decentralized and immutable nature empowers cloud computing services to establish secure and private data interactions. By leveraging blockchain's consensus mechanism, we demonstrate the feasibility of creating a robust platform for authenticating transactions involving digital assets. Through cryptographic methods, blocks of transactions are securely linked, ensuring data integrity. This paper provides a roadmap for understanding security concerns in cloud computing and offers insights into the potential of blockchain technology. We conclude by outlining future research directions that can drive innovation in this exciting intersection of fields.**

***Keywords*—Cloud computing; security; blockchain; review**

I. INTRODUCTION

Cloud computing has gained considerable attention in recent years owing to its affordability, sustainability, reliability, scalability, and flexibility. Under a pay-per-use model, it provides on-demand access to infinite virtual resources such as computing, storage, and networks [1]. This scalable and flexible approach to resource delivery has attracted many organizations and individuals. Cloud computing has enabled many enterprises to migrate, compute, and host their applications, giving them seamless access to a range of services without hassle [2]. It is reported that approximately 60 percent of organizations use cloud services to meet their resource needs, accounting for nearly 15 percent of global IT spending [3]. The cloud can efficiently manage bursts of heterogeneous data. It serves as a bridge between end users and the middleware of devices within the IoT architecture [4]. There is a great deal of concern about security in the cloud, which encompasses power consumption, product lifespan, and overall performance [5]. CCTV cameras, social media, and other cloud devices can be accessed and compromised in public places. A Brute Force attack has been conducted on the cloud application due to a weak authentication scheme [6].

The complexity of the cloud computing model and the shared technologies have raised security concerns despite the obvious benefits [7]. Several elements are involved in the cloud paradigm, such as the network, architecture, APIs, and hardware, which increases the complexity of security issues [8]. This may result in security vulnerabilities if a cloud provider or client uses different configurations. While cloud computing offers organizations benefits such as cost savings, measurable services, rapid scalability, and elasticity, it also introduces inherent risks that must not be overlooked. Cloud computing systems inherently possess various vulnerabilities, giving rise to significant security concerns [9]. Organizations may hesitate to adopt cloud computing despite its potential if they lack robust security policies. An illustration of the advantages of cloud computing can be found in Fig. 1.

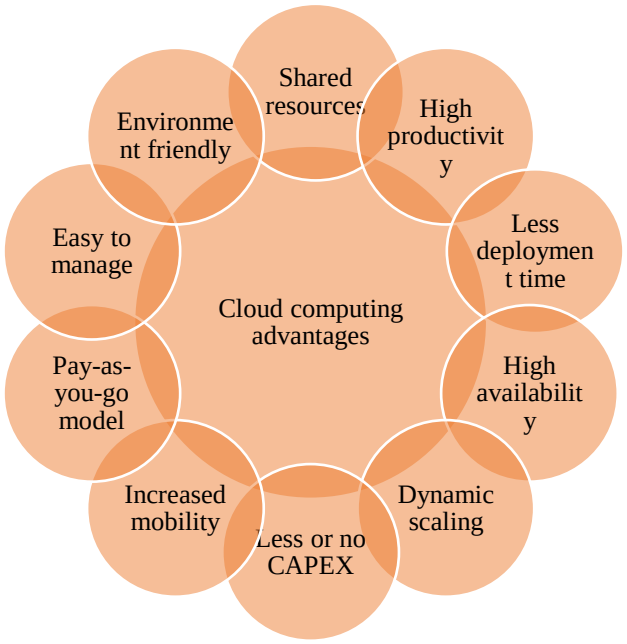

Fig. 1. Cloud computing advantages

Cloud computing offers users on-demand access to customized computing resources, such as services, applications, storage, and servers; instantly delivered by a service provider requiring little management effort. This allows users to access the latest technologies and to scale resources up or down quickly and easily, depending on their needs [10]. It also reduces the costs associated with software and hardware purchases and maintenance. Fig. 2 illustrates four ways cloud

computing can be implemented: public, private, community, and hybrid. In its simplest form, a public cloud is a cloud environment that is publicly accessible by a large number of cloud customers without any restrictions imposed by the cloud provider. Private cloud environments offer the same advantages as public clouds, but access is limited to a specific user or organization. Community clouds provide a shared cloud environment for a specific group of users and organizations. Hybrid clouds combine public and private clouds, offering more flexibility and scalability [11].

Cloud computing encompasses three main service types: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS allows users to access applications hosted in the cloud, while PaaS offers a platform for developing, running, and managing applications. IaaS, on the other hand, provides the necessary infrastructure, including servers and storage, to run applications. Cloud computing is characterized by key attributes: measured service, rapid elasticity, resource pooling, broad network access, and on-demand self-service [12]. Several metrics can be used to quantify cloud services, including bandwidth, data, and time. Cloud computing services are typically priced according to the number of resources used, and when compared to traditional IT solutions, these services can result in significant cost savings [13]. In cloud computing, the concept of elasticity is used to describe the ability of the system to respond to changes in workloads through automatic provisioning and de-provisioning, as well as the availability of resources. Resource pooling involves pooling virtual and physical resources and allocating and reallocating them dynamically according to consumer demand in a multitenant environment. Broad network access refers to the ability to locate and access resources on a network using various devices and computing platforms, such as tablets, smartphones, laptops, and desktop computers. In the context of on-demand self-service, users have access to their data and resources in the cloud whenever they need them without requiring assistance from a human [14].

Artificial intelligence (AI) and machine learning (ML) play a pivotal role in the synergy of blockchain-enabled cloud computing, ushering in new frontiers of efficiency and security. AI algorithms leverage the immense volumes of data stored in the blockchain to uncover insights, predict patterns, and optimize resource allocation within cloud systems. ML algorithms enhance consensus mechanisms by dynamically adapting to network demands and mitigating latency [15, 16]. Moreover, AI-driven anomaly detection and threat analysis fortify cloud security by identifying and preemptively mitigating potential breaches. This amalgamation empowers cloud computing with self-optimizing capabilities and real-time threat response, elevating the potential for creating resilient and adaptive cloud ecosystems that harness both the transparency of blockchain and the intelligence of AI and ML [17].

Blockchain technology's potential to address security and performance challenges within distributed systems has garnered significant attention. Integrating blockchain presents a compelling avenue for innovation in the context of cloud computing, which necessitates robust security measures and efficient data management. While existing literature acknowledges the potential of blockchain in enhancing cloud security, a thorough examination of the distinctive security issues and recent advancements in this intersection remains limited. To bridge this gap, our work offers a comprehensive taxonomy of security concerns specifically tailored to blockchain-enabled cloud computing. Beyond traditional gap analyses, we delve into the nuanced intricacies of how blockchain uniquely tackles security and data integrity concerns within the cloud environment. Furthermore, we present an in-depth review of recent advancements that leverage blockchain to reinforce cloud computing's security framework.

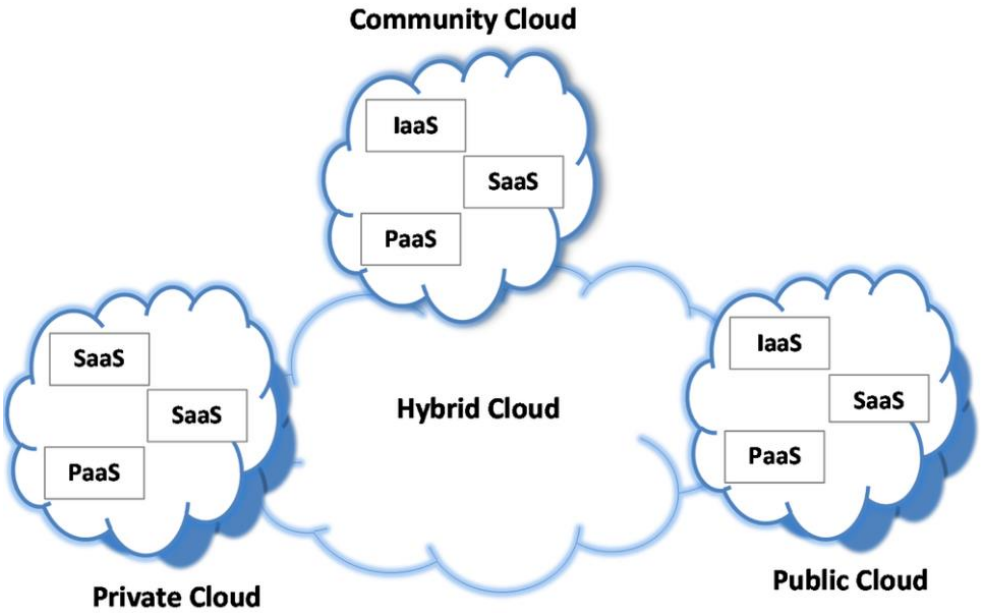

Fig. 2. Cloud deployment models and infrastructure.

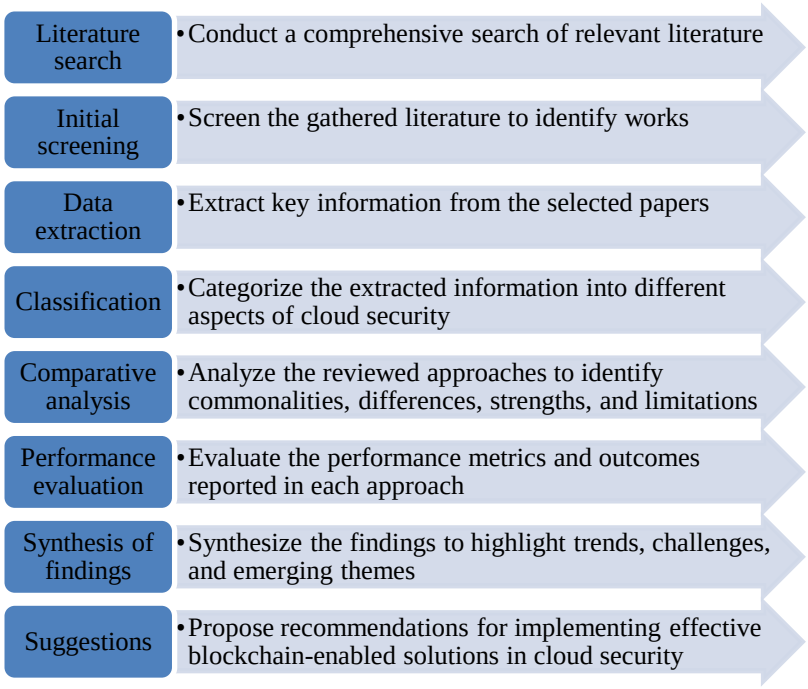

Fig. 3. Review process for blockchain-enabled cloud security approaches.

To systematically review and assess blockchain-enabled cloud security approaches, we have developed a block diagram that illustrates the step-by-step process (See Fig. 3). Beginning with a comprehensive literature search (Step 1), relevant sources are identified and screened (Step 2) to extract key information from selected papers (Step 3). This information is then classified into various aspects of cloud security, such as data integrity and access control (Step 4). A comparative analysis (Step 5) highlights commonalities and differences among the reviewed approaches. Performance evaluation (Step 6) is a crucial element wherein metrics like scalability and efficiency are assessed. The synthesis of findings (Step 7) allows us to outline trends, challenges, and emerging themes in blockchain-enabled cloud security. Moreover, the diagram visualizes the identification of new blockchain solutions (Step 8) that address gaps in existing literature. Lastly, recommendations (Step 9) for the implementation of effective blockchain solutions in cloud security conclude the process. This block diagram visually represents our rigorous approach to evaluating and enhancing cloud security through blockchain integration.

The remainder of the paper is organized in the following manner. Section II delves into a comprehensive review of existing literature on cloud computing security. Section III focuses on our analysis of blockchain technology's potential in enhancing cloud security. Section IV presents our research findings. Section V concludes the paper.

II. Literature Review

Cloud security plays a crucial role in safeguarding all layers of computing in both public and private clouds. As illustrated in Fig. 4, cloud applications benefit from three levels of protection: SaaS, PaaS, and IaaS. This study focuses on analyzing the existing challenges associated with cloud security and exploring the latest advancements in security solutions. It aims to provide insights into the evolving landscape of cloud security and identify effective measures to mitigate risks and protect cloud-based applications. There are 28 security problems described in the article that can be categorized into five groups (Table I). Comparative evaluations can also be conducted on the latest security technologies and countermeasures. Table I summarizes five types of cloud computing safety concerns. In [10], the same method is used to classify problems, but only for small groups and not for all four types.

Fig. 5 provides an overview of potential security risks associated with different components of the cloud. The cloud infrastructure, clients, and network are all vulnerable to security threats, necessitating the implementation of preventive, detective, and responsive strategies. Table I categorizes these components according to their respective cloud security categories. To enhance security, various security specifications such as SSL, TLS, XML signatures, Interoperability key management protocols, and XML Encryption Syntax and Processing are necessary. Currently, there is a lack of widely accepted security standards specific to cloud computing. While safety requirements may be appropriately defined, compliance risks significantly impact several security issues. The absence of effective governance and evaluation of corporate standards exacerbates this problem. In particular, cloud clients often lack sufficient knowledge regarding the provider's protocols, processes, and activities, particularly in the areas of identity management and job separations.

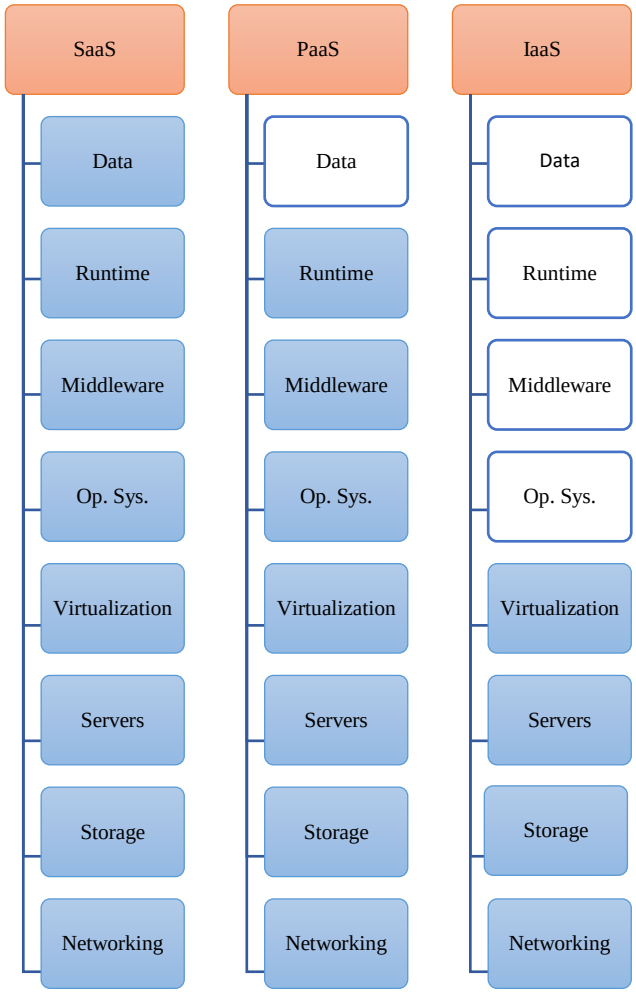

Fig. 4. Cloud security aspects

TABLE I. A TAXONOMY OF CLOUD SECURITY ISSUES

Group	Description	Issues
Data	It addresses data storage, privacy, and data migration issues concerning data security.	Accessibility, protection, privacy, recovery, placement, data loss, and redundancy information
Cloud infrastructure	It focuses on specific threats related to cloud infrastructure	QoS, server location and backup, security misconfiguration, multi-tenancy, reliability of suppliers, and sharing of technical faults
Access control	It is concerned with authentication and connectivity issues and identifies concerns regarding user privacy and data storage.	Browser protection, malicious insider, privileges of the user, and authentication mechanism
Network	It encompasses network intrusions such as link access, DDoS, DoS, flooding attacks, and bugs in the IP protocol.	Installation of the right network firewalls, Internet dependence, IP vulnerabilities, and network security configuration
Security standards	It clarifies the requirements for cloud storage as well as preventive measures to prevent unauthorized access. It specifies cloud computing safety regulations without compromising reliability and efficiency.	Inadequacies in security standards, legal issues, audit failures, enforcement risks, and trust

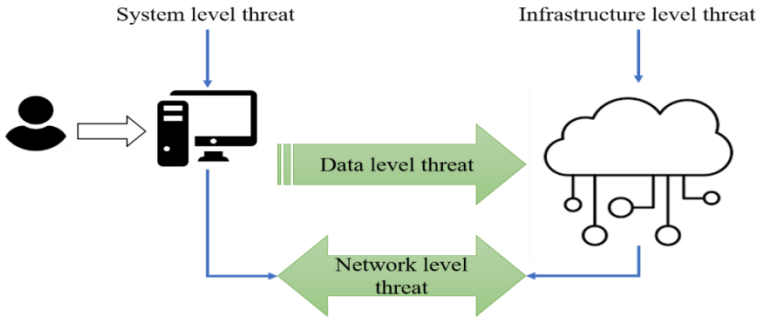

Fig. 5. Security threats associated with cloud components.

The audibility of cloud computing is one of its most critical features. However, there is no network of audit providers for cloud computing services. Ensuring auditability is crucial when a service provider outsources a non-transparent service. It is essential that the entire process is auditable to maintain transparency and accountability. However, security standards and governing bodies that protect Service Level Agreements (SLAs) and regulatory matters are not currently incorporated into cloud computing practices. This absence of established security standards and governing bodies poses challenges in effectively addressing and mitigating risks associated with outsourced services in cloud computing environments. Considering the vulnerability of cloud computing to network-related security attacks, network problems pose the greatest threat to cloud security. Operations in the cloud are heavily dependent on networking and are closely interconnected. The quality of service (QoS) has emerged as an unexpected challenge in the cloud computing landscape, as numerous service providers aim to offer fast and cost-effective performance. We consider QoS to be a critical factor that directly or indirectly influences security. Even a minor error in the configuration of one or more cloud components can have a profound impact on multiple services, considering that cloud configurations are often shared among numerous services. Various case studies emphasize the significance of encrypting, securing, managing, and ensuring timely access to data. This highlights the importance of addressing QoS concerns to ensure the overall security and effectiveness of cloud computing services. Several issues have been identified as major concerns in the literature, including data availability [18], data security [19], data confidentiality [20], data recovery [21], data localization [22], data loss [9], and data redundancy [23].

Blockchain technology refers to a network of blocks containing user records safeguarded using cryptography. These blocks are interconnected, allowing for the distribution of information throughout the network. The concept of blockchain was initially introduced in 1991 by Stuart Haber and W Scott Stornetta [24]. It was later implemented by an anonymous developer known as Satoshi Nakamoto, who used it in the creation of the digital currency Bitcoin. Initially designed for Bitcoin, blockchain technology has now found applications in various domains. Researchers have explored its potential in securing financial transactions, contracts, inter-organizational transactions, IoT systems, banking, land records, and more. Bitcoin's success in maintaining distributed ledgers and transactions without the involvement of a central authority has been instrumental in advancing blockchain technology. While Bitcoin continues to operate on Nakamoto's original blockchain, other projects like Ethereum and Ripple have emerged, each with its own set of rules and regulations and a wider range of applications [25].

Decentralization, transparency, and immutability are three characteristics of blockchain. Decentralization entails that the blockchain distributes its contents, which means the blockchain does not have a single owner. Transparency indicates that transaction information can be viewed only by a user's public address. A blockchain cannot be modified due to its immutability. These characteristics create an immutable and secure network resistant to hacking and tampering. The transactions stored on the blockchain cannot be reversed and are fully traceable. The distributed nature of the blockchain also allows data to be stored securely and reliably [26].

Fig. 6 provides an illustration of the structure of blockchain and its associated technologies. A block is composed of two main components: the header and the transactions. The header contains the hash value of the previous block and a unique nonce number. The transactions part contains information about all the transactions included in the block. Each block includes the hash value of the previous block, which is a combination of the previous block's hash value and the current block's hash value. This property ensures the immutability of the blockchain. If an attacker attempts to modify the hash value by even a single bit, it will result in a change in the hash value of the subsequent block. This ripple effect continues throughout the entire blockchain. The attacker would need to recalculate the hash value of all the following blocks, which is extremely challenging.

Blockchain technology enables various applications in fields such as healthcare, finance, distribution, and more. One of the key features of blockchain is its ability to facilitate peer-to-peer transactions without the need for a centralized authority. The foundation of blockchain technology is built upon principles of trust and security, which are enabled through cryptography. By establishing peer-to-peer communication within a decentralized network, blockchain technology allows for trust to be established among unknown peers. The use of public and private keys plays a crucial role in ensuring security within the blockchain. A public key serves as a shared address known to everyone in the network, similar to an email address. On the other hand, a private key is a unique address that is only accessible to the user, similar to an email password.

Software programmers play a crucial role in verifying and validating transactions on the blockchain. To enhance and streamline transactions, innovative technologies have been incorporated into the computational elements of the blockchain. These transactions are recorded in a distributed ledger to ensure transparency and immutability. While blockchain technology is integral to modern digital systems, it does have certain limitations. The small size of blocks restricts the number of transactions that can occur within the network, leading to longer block creation times and reduced throughput. Fig. 7 provides an overview of the transactional flow in blockchain technology. Nodes serve as the foundation of blockchain architecture, with users or highly configured computers acting as nodes. Each node maintains a complete copy of the blockchain ledger. Miners, which are specialized nodes, have the capability to add new blocks to the blockchain. Users undergo authentication, verification, and validation processes by miners. Once a transaction is authenticated and validated by miners, the corresponding amount is deducted from the sender's wallet and credited to the receiver's wallet. The concept of a block can be likened to a container that holds an aggregated set of transaction details. New transactions initiated on the blockchain result in the creation of a new block, which can only be added to the blockchain after successful verification by miners.

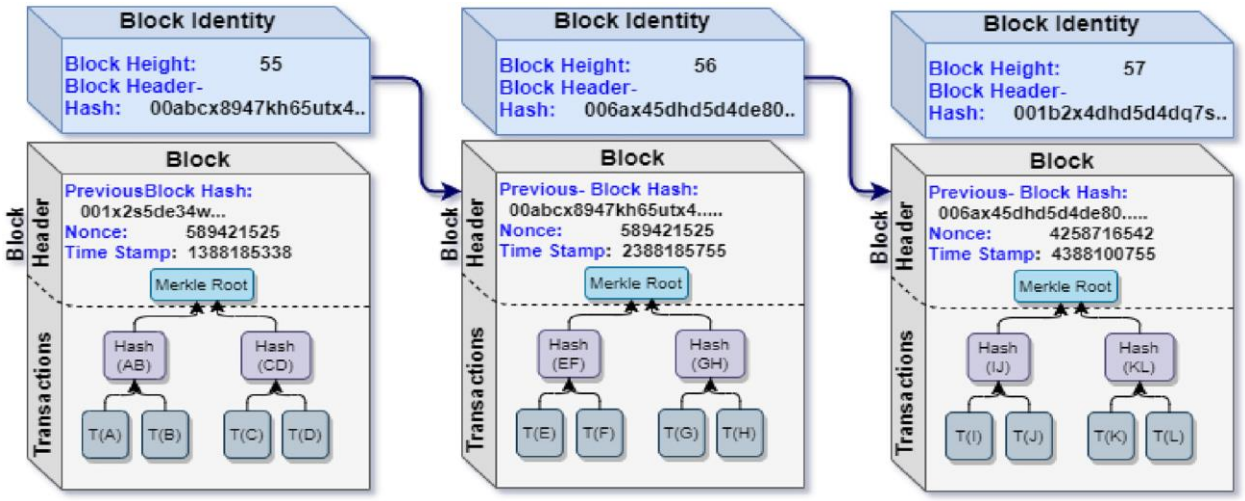

Fig. 6. Blockchain structure.

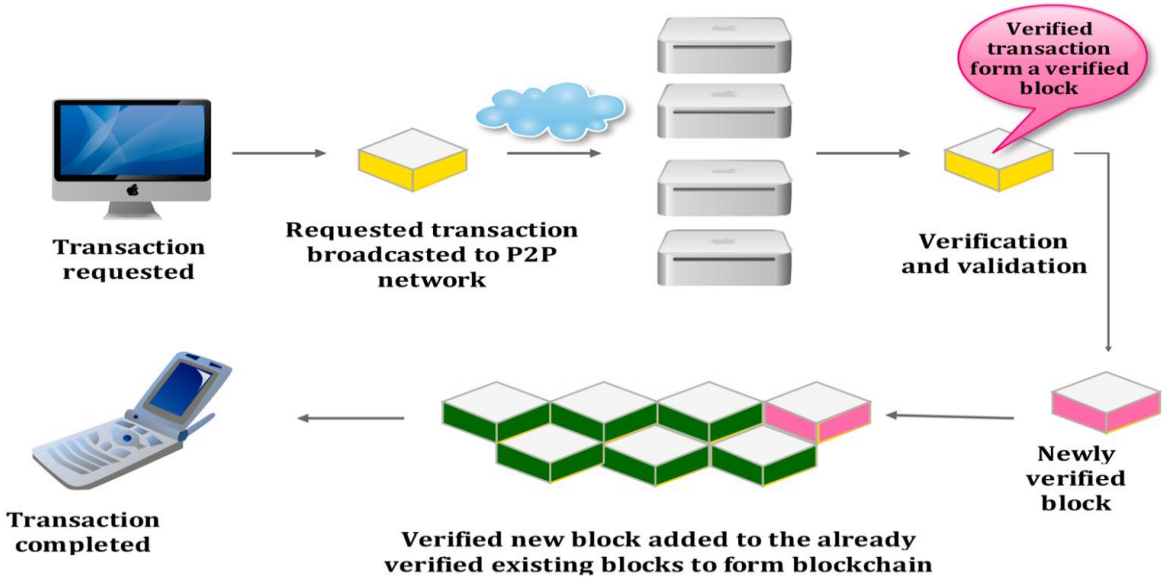

Fig. 7. Transaction flow blockchain technology.

III. Blockchain-enabled Cloud Security Approaches

Blockchain technology and smart contracts have impacted a wide range of engineering and computer science disciplines. Cloud computing can benefit from blockchain technology by re-engineering the data centers. Due to its decentralized operating model, blockchain can potentially replace centralized cloud-based services. Blockchain has the potential to become a critical component of cloud systems due to its minimal costs and management overhead. It has been used in recent research to establish security and confidence in cloud-based applications. There are several challenges associated with the integration of blockchain technology and cloud computing:

- Blockchain was founded on the principle of decentralization in contrast to the cloud, which is entirely managed centrally and provides minimal transparency and trust configurations. Since various legal and governmental reasons make it impossible to eliminate centralization, it is necessary to adopt a hybrid strategy whereby the cloud provider maintains some level of control while maintaining trust and transparency with the cloud users.
- Cloud data is protected from unauthorized access, while blockchain data is freely accessible. Cloud services based on blockchain technology will be widely adopted due to privacy concerns.
- Unlike cloud systems, blockchain systems are inherently susceptible to scaling problems.

The integration of blockchain technology with cloud-based services is urgently needed despite the mentioned issues. However, the question remains of how to integrate blockchain technology with the cloud. A cloud computing business model is attractive because of outsourcing services, but users and outsourcing service providers distrust one another. Zhang, et al. [27] developed the BCPay framework for fair payment for

outsourcing services in cloud computing, which achieves soundness and robustness. The system is also highly efficient regarding transaction volume and computational costs. Velmurugadass, et al. [28] developed a cloud-based Software Defined Network (SDN) for monitoring data and evidence-related operations. The SDN controller employs a blockchain system in order to protect the evidence gathered through data and user signatures. Using the Logical Graph of Evidence (LGoE), the investigator generates a report, evaluates the evidence, retrieves the evidence, and identifies the evidence. Using the evidence provided by the controller, the investigator can construct a Logical Graph of Evidence (LGoE).

Wilczyński and Kołodziej [29] proposed a blockchain-based cloud scheduler model. This model has improved the effectiveness of preparing schedules, and the simulator returns a schedule with a shorter makespan than previous individual scheduling methods. Using blockchain technology, Li, et al. [30] proposed a robust, cost-aware data caching strategy that minimizes the possibility of cache data tampering. To address trust issues between consumers, sellers, and agents, Rahman, et al. [31] propose a new exchange scheme combining blockchain with SDN to address the security risks associated with cloud computing. Distributed blockchain networks securely enable data storage and transmission, allowing scalability, flexibility, and privacy. Blockchain technology also ensures the security and privacy of data, while maintaining the system's integrity.

In order to monitor the activities of users and administrators, an audit log is essential. Still, it is susceptible to manipulation if an attacker can access the system. Attackers may modify and delete log entries or even create false entries to cover their tracks. Managing audit logs requires the protection of these records from unauthorized access. Keeping the log in a secure location with restricted access and recording and monitoring all access is essential to prevent unauthorized access.

Furthermore, the log should be regularly backed up and stored in a secure offsite location in order to detect and correct any modifications or deletions. Using blockchain technology, Ali, et al. [32] propose a Log Management System that addresses several limitations. Functionality and performance were superior to those of previous models. Xu, et al. [33] have introduced a blockchain-based method for managing cloudlets in a multi-media workflow. A multi-media application is enhanced using NSGA III, and an optimal scheduling decision is made using ELECTRE. Eltayieb, et al. [34] developed a cloud-based data-sharing platform based on blockchain technology coupled with attribute-based sign encryption. The proposed scheme complies with the security requirements of cloud computing, including confidentiality and unforgeability. The smart contract also eliminates the problem with traditional cloud servers, such as returning incorrect results.

Awadallah and Samsudin [35] introduced a cloud relational database with an enhanced structure based on blockchain technology. The client has the ability to detect and prevent errors in cloud relational database manipulation by employing a self-verification mechanism. They proposed two systems for improving the mechanism's performance: an agile blockchain-based cloud relational database and a secure blockchain-based cloud relational database. Byzantine fault tolerance distributes both systems across several cloud service providers. The SHA-256 algorithm is also used in both systems to link records. In addition, blockchain-based cloud relational databases that operate on a proof-of-work consensus prevent data offensive operations. A blockchain-based cloud relational database is highly recommended for high throughput databases based on performance and security analysis. Cloud relational databases based on blockchain technology are recommended for containing sensitive data and performing poorly in terms of throughput. The flexibility of cloud-based relational databases allows users to operate them according to their specific requirements.

Intrusion Detection System (IDS) has become widely recognized as a valuable tool for protecting networks and information. IDS monitors network traffic and alerts administrators when malicious activities or suspicious behavior is detected. It is used to detect and prevent any unauthorized access or malicious attacks. Host IDS (HIDS) detects unauthorized use and abnormal and malicious activity on a host, whereas Network IDS (NIDS) detects network attacks and intrusions. Kumar and Singh [36] propose the development of Distributed IDS (DIDS) based on emerging and promising technologies like blockchain on a stable platform such as cloud infrastructure.

Access control is of paramount importance in cloud computing, as it is where enterprises and individuals store their sensitive data. However, the centralized access control mechanism used in the cloud poses a significant security risk. Sensitive data stored in the cloud becomes vulnerable to tampering or unauthorized disclosure by hackers or even cloud managers. This highlights the need for robust access control technologies to ensure the confidentiality and integrity of data in the cloud environment. To address this issue, Yang, et al. [37] propose AuthPrivacyChain, a blockchain-based access control framework with privacy protection. The first step is to use the account address of a node in the blockchain as the identity and simultaneously redefine the permissions for access control to the cloud. They then design processes for controlling access, authorizing users, and revoking authorizations. Lastly, the researchers implement AuthPrivacyChain using the enterprise operation system (EOS) and evaluate its performance. The results demonstrate that AuthPrivacyChain offers robust protection against unauthorized access by hackers and administrators. Additionally, it ensures the preservation of authorized privacy, providing a comprehensive security solution.

IV. DISCUSSION

In this section, we present and analyze the findings of our research on blockchain-enabled cloud security solutions. Our investigation, encompassing a systematic literature review and analysis, revealed several key insights that contribute to the evolving understanding of this field.

Cloud service users have high expectations from cloud service providers in terms of transparency, efficiency, security, and authentication of transactions, services, and applications. Trust and credibility in cloud network transactions depend on involving a trusted third party to verify, validate, and endorse

them. Incorporating business logic into the database (Ledger) and executing it becomes necessary for transaction validation and storage. Blockchain technology, with its inherent capabilities and potential, holds the promise of addressing many of the challenges faced by virtualized cloud infrastructures today. It offers secure, transparent, trustworthy, and efficient solutions for managing and registering the authorized identities of all stakeholders in the cloud. Its decentralized and distributed nature, coupled with a reliable management and governance system, allows for tracking, tracing, and effective management of cloud-related transactions. Additionally, blockchain can be leveraged to manage and store identities and services, ensuring their complete concealment from end users.

Cloud infrastructures can be made more secure by integrating blockchain technology. Oracle Blockchain Cloud Service is one example of a blockchain-enabled cloud solution currently being implemented. A virtualized cloud environment can also benefit from the use of blockchain technology. All connected cloud devices and services can be registered and identified on the blockchain ledger through a set of attributes and complex relationships. Consequently, virtualized cloud supply chain networks can provide provenance at all levels. Cloud-enabled supply chains involve numerous stakeholders, ranging from cloud infrastructure facilities, vendors, suppliers, and service providers to distributors, shippers, installers, owners, repairers, and re-installers. Anonymity is a key aspect in large-scale cloud environments. To ensure privacy and prevent third-party service providers from accessing private information, an electronic wallet is created and installed within cloud systems. Furthermore, blockchain-enabled smart contracts play a crucial role in managing, controlling, and securing cloud services and devices. The previous section highlighted the significant features of blockchain technology that are particularly valuable for cloud platforms, especially in terms of enhancing cloud security.

A virtualized cloud system offers anonymity for user information and service data, which can be strengthened by integrating blockchain-enabled solutions. One such solution is the implementation of electronic wallets within large-scale cloud environments, which utilize blockchain platforms to store users' and services' data securely. By leveraging a blockchain network, cloud service records can be stored, and the identities of cloud users and service providers can be authenticated and validated. This combination of virtualized cloud systems and blockchain technology provides an additional layer of security and trust in cloud-based transactions and interactions. Whenever a cloud service provider connects to a blockchain network, it will prove and sign its transactions cryptographically, which can be tracked and tracked by users or cloud service providers participating in the network. A blockchain-based smart contract ensures user and service privacy by controlling who has permission to update, upgrade, patch, provide new key pairs, initiate a service or repair request, and change ownership. The blockchain network provides fault tolerance and resilience to cloud users, as the failure of a single node will not affect the entire virtualized cloud infrastructure. By integrating blockchain into a cloud infrastructure solution, blockchain-as-a-service (BaaS) can be implemented. BaaS allows users to leverage the advantages of blockchain technology without having to build an entire infrastructure from scratch. It also provides a secure platform for cloud services, and users can manage, monitor, and control their data easily. Additionally, BaaS can enable cost and time savings for businesses. Furthermore, BaaS enables businesses to scale quickly and efficiently while providing a secure and reliable platform.

Several key findings have emerged from our comprehensive exploration of blockchain-enabled cloud security approaches. Through a systematic review of the literature, we categorized and analyzed various mechanisms that leverage blockchain technology to enhance the security of cloud computing environments. Our investigation revealed that these mechanisms encompass data integrity verification, access control, consensus protocols, and auditability. These findings underscore the potential of blockchain technology to offer innovative solutions for addressing the unique security challenges inherent in cloud environments. Comparing our findings with those of previous studies, our research aligns with the insights presented by AlMuraytib, et al. [38]. Both studies highlight the potential of blockchain to enhance cloud security by ensuring data integrity and enhancing trust in cloud transactions. While we echo these sentiments, our study goes further by delving deeper into the distinct security challenges that cloud computing faces and presenting novel mechanisms specifically designed to tackle these issues. Our focus on tailoring blockchain solutions to address the intricacies of cloud security sets our work apart and contributes a fresh perspective to the field. Furthermore, our research contributes a domain-specific understanding of how blockchain principles can be adapted to meet the security demands of cloud computing. While existing studies primarily emphasize the application of general blockchain principles, our work recognizes the need for nuanced approaches to accommodate the intricacies of cloud environments. By doing so, we bridge a critical gap in the literature and offer a more targeted and effective path toward securing cloud-based systems.

V. CONCLUSION

This paper discussed the potential for transformation that arises from integrating blockchain technology with cloud computing, focusing on overcoming major security and performance challenges. The study highlighted the diverse benefits that this combination brings to the field of information technology. The initial phase of our investigation was identifying security concerns inherent in cloud computing. The need to protect data integrity arises from the vulnerability to data modification and compromise, hence requiring the development of novel solutions. Blockchain technology, known for its robust resistance to tampering, is a valuable strategic partner in this context. The originality of our study is in the application of blockchain technology specifically tailored to address security concerns in cloud computing. In contrast to prior research that use broad concepts, our research emphasizes customizing blockchain solutions to address the complexities of cloud computing, showcasing novel processes. The procedures above encompass data integrity verification, access control, and consensus protocols, effectively target and mitigate security vulnerabilities. The research findings have

far-reaching ramifications for both the academic community and several industries. By providing practitioners and researchers with security solutions tailored to certain domains, we improve the reliability of transactions conducted in cloud-based environments. Incorporating blockchain technology facilitates improving data quality and dependability, which is a crucial need in several application fields. As we contemplate the future, the convergence of cloud computing and blockchain technology presents significant possibilities. The secure and efficient data storage and processing offer potential competitive benefits for firms. The trajectory forward necessitates more investigation in order to fully elucidate the comprehensive range of repercussions stemming from this fusion. This discovery signifies the advent of a hopeful era in which cloud computing is strengthened by the powerful security framework of blockchain, leading to a trajectory towards a digital landscape that is more safe and efficient.

REFERENCES

[1] B. Pourghebleh, A. A. Anvigh, A. R. Ramtin, and B. Mohammadi, "The importance of nature-inspired meta-heuristic algorithms for solving virtual machine consolidation problem in cloud environments," Cluster Computing, pp. 1-24, 2021.

[2] F. Nzanywayingoma and Y. Yang, "Efficient resource management techniques in cloud computing environment: a review and discussion," International Journal of Computers and Applications, vol. 41, no. 3, pp. 165-182, 2019.

[3] D. C. Wyld, Moving to the cloud: An introduction to cloud computing in government. IBM Center for the Business of Government, 2009.

[4] B. Pourghebleh and N. J. Navimipour, "Data aggregation mechanisms in the Internet of things: A systematic review of the literature and recommendations for future research," Journal of Network and Computer Applications, vol. 97, pp. 23-34, 2017.

[5] L. Jayashree, G. Selvakumar, L. Jayashree, and G. Selvakumar, "Cloud Solutions for IoT," Getting Started with Enterprise Internet of Things: Design Approaches and Software Architecture Models, pp. 31-48, 2020.

[6] M. M. Salim, S. K. Singh, and J. H. Park, "Securing Smart Cities using LSTM algorithm and lightweight containers against botnet attacks," Applied Soft Computing, vol. 113, p. 107859, 2021.

[7] V. Hayyolalam, B. Pourghebleh, and A. A. Pourhaji Kazem, "Trust management of services (TMoS): Investigating the current mechanisms," Transactions on Emerging Telecommunications Technologies, vol. 31, no. 10, p. e4063, 2020.

[8] V. Hayyolalam, B. Pourghebleh, A. A. P. Kazem, and A. Ghaffari, "Exploring the state-of-the-art service composition approaches in cloud manufacturing systems to enhance upcoming techniques," The International Journal of Advanced Manufacturing Technology, vol. 105, no. 1-4, pp. 471-498, 2019.

[9] M. E. Hussain and R. Hussain, "Cloud Security as a Service Using Data Loss Prevention: Challenges and Solution," in Internet of Things and Connected Technologies: Conference Proceedings on 6th International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2021, 2022: Springer, pp. 98-106.

[10] A. Hedhli and H. Mezni, "A survey of service placement in cloud environments," Journal of Grid Computing, vol. 19, no. 3, pp. 1-32, 2021.

[11] D. Hazra, A. Roy, S. Midya, and K. Majumder, "Energy aware task scheduling algorithms in cloud environment: A survey," in Smart Computing and Informatics: Springer, 2018, pp. 631-639.

[12] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration," ACM Computing Surveys (CSUR), vol. 51, no. 6, pp. 1-29, 2019.

[13] E. J. Ghomi, A. M. Rahmani, and N. N. Qader, "Load-balancing algorithms in cloud computing: A survey," Journal of Network and Computer Applications, vol. 88, pp. 50-71, 2017.

[14] L. M. Dang, M. Piran, D. Han, K. Min, and H. Moon, "A survey on internet of things and cloud computing for healthcare," Electronics, vol. 8, no. 7, p. 768, 2019.

[15] T. Gera, J. Singh, A. Mehbodniya, J. L. Webber, M. Shabaz, and D. Thakur, "Dominant feature selection and machine learning-based hybrid approach to analyze android ransomware," Security and Communication Networks, vol. 2021, pp. 1-22, 2021.

[16] S. N. H. Bukhari, J. Webber, and A. Mehbodniya, "Decision tree based ensemble machine learning model for the prediction of Zika virus T-cell epitopes as potential vaccine candidates," Scientific Reports, vol. 12, no. 1, p. 7810, 2022.

[17] J. Webber, A. Mehbodniya, Y. Hou, K. Yano, and T. Kumagai, "Study on idle slot availability prediction for WLAN using a probabilistic neural network," in 2017 23rd Asia-Pacific Conference on Communications (APCC), 2017: IEEE, pp. 1-6.

[18] C. B. Tan, M. H. A. Hijazi, Y. Lim, and A. Gani, "A survey on proof of retrievability for cloud data integrity and availability: Cloud storage state-of-the-art, issues, solutions and future trends," Journal of Network and Computer Applications, vol. 110, pp. 75-86, 2018.

[19] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: A survey," IEEE Access, vol. 8, pp. 131723-131740, 2020.

[20] M. Rady, T. Abdelkader, and R. Ismail, "Integrity and confidentiality in cloud outsourced data," Ain Shams Engineering Journal, vol. 10, no. 2, pp. 275-285, 2019.

[21] T. Wang, Q. Yang, X. Shen, T. R. Gadekallu, W. Wang, and K. Dev, "A privacy-enhanced retrieval technology for the cloud-assisted internet of things," IEEE transactions on industrial informatics, vol. 18, no. 7, pp. 4981-4989, 2021.

[22] V. Inđić, M. Kovačević, M. Simić, and G. Sladić, "Towards Local Cloud Infrastructure in Developing Countries as a Response to Data Localization Regulations," ed: ICIST, 2022.

[23] S. Mohapatra, N. Bajpai, T. Swarnkar, and M. Mishra, "Raw Data Redundancy Elimination on Cloud Database," in Computational Intelligence in Pattern Recognition: Proceedings of CIPR 2020, 2020: Springer, pp. 395-405.

[24] J. Doyle, M. Golec, and S. S. Gill, "Blockchainbus: A lightweight framework for secure virtual machine migration in cloud federations using blockchain," Security and Privacy, vol. 5, no. 2, p. e197, 2022.

[25] A. Alkhateeb, C. Catal, G. Kar, and A. Mishra, "Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review," Sensors, vol. 22, no. 4, p. 1304, 2022.

[26] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," Neural Computing and Applications, pp. 1-16, 2021.

[27] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," Information Sciences, vol. 462, pp. 262-277, 2018.

[28] P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan, "Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," Materials Today: Proceedings, vol. 37, pp. 2653-2659, 2021.

[29] A. Wilczyński and J. Kołodziej, "Modelling and simulation of security-aware task scheduling in cloud computing based on Blockchain technology," Simulation Modelling Practice and Theory, vol. 99, p. 102038, 2020.

[30] C. Li, S. Liang, J. Zhang, Q.-e. Wang, and Y. Luo, "Blockchain-based data trading in edge-cloud computing environment," Information Processing & Management, vol. 59, no. 1, p. 102786, 2022.

[31] A. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, and P. Tiwari, "Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT," Digital Communications and Networks, 2022.

[32] A. Ali, A. Khan, M. Ahmed, and G. Jeon, "BCALS: Blockchain-based secure log management system for cloud computing," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 4, p. e4272, 2022.

[33] X. Xu, Y. Chen, Y. Yuan, T. Huang, X. Zhang, and L. Qi, "Blockchain-based cloudlet management for multi-media workflow in mobile cloud

computing," Multi-media Tools and Applications, vol. 79, pp. 9819-9844, 2020.

[34] N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud," Journal of Systems Architecture, vol. 102, p. 101653, 2020.

[35] R. Awadallah and A. Samsudin, "Using blockchain in cloud computing to enhance relational database security," IEEE Access, vol. 9, pp. 137353-137366, 2021.

[36] M. Kumar and A. K. Singh, "Distributed intrusion detection system using blockchain and cloud computing infrastructure," in 2020 4th international conference on trends in electronics and informatics (ICOEI)(48184), 2020: IEEE, pp. 248-252.

[37] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud," IEEE Access, vol. 8, pp. 70604-70615, 2020.

[38] S. AlMuraytib, L. Alqurashi, and S. Snoussi, "Blockchain-based solutions for Cloud Computing Security: A Survey," in Proceedings of the 6th International Conference on Future Networks & Distributed Systems, 2022, pp. 338-342.