OIC-CERT Journal of Cyber Security
Volume 5, Issue 1 (July 2024)
1 - 10

Cloud Security Maturity Index to Measure the Cybersecurity Maturity Level of Cloud Service Providers in Indonesia

Raden Budiarto Hadiprakoso[1], Hermawan Setiawan[2], I Komang Setia Buana[3]
Herman Kabetta[3], Rahmat Purwoko[4], and Amiruddin[5]
[1-6] State Cyber and Crypto Agency, Jakarta, Indonesia
budiarto.hadiprakoso@bssn.go.id[1], hermawan.setiawan@bssn.go.id[2]
komang.setia@bssn.go.id[3], herman.kabetta@bssn.go.id[4]
rahmat.purwoko@bssn.go.id[5], amiruddin@bssn.go.id[6]

ARTICLE INFO

Article History
Received 31 Jan 2023
Received in revised form 31 Jan 2024
Accepted 20 Mar 2024

Keywords:
Cloud security; cloud security government; KAMI index; maturity model; cloud-security framework

ABSTRACT

Cyberspace has an impact on every aspect of our lives. *Cloud computing* is a innovative cyberspace technology that has established itself as one of the essential resource-sharing platforms for forthcoming on-demand infrastructures and services that enable the internet of things, big data, and software-defined systems/services. Security is more important than ever in a cloud environment. Numerous cloud security models and standards are in place to deal with emerging cloud security concerns. However, these models are primarily reactive rather than initiative-taking and do not give suitable measures to analyze a cloud system's overall security posture. Capability maturity models, which many companies have utilized, provide a practical method to address these issues through management by security domains and security evaluation based on maturity levels. The paper has two goals: first, it provides a review of cyber security, cloud security models and standards, cyber security capability maturity models, and security metrics; second, we propose a cloud security maturity index (CSMI) that extends existing information security models (KAMI index) with a security metric framework. CSMI seeks to provide senior management with a reliable overall security evaluation of a cloud system and to enable security professionals to foresee and identify essential security solutions.

I. INTRODUCTION

The cloud has emerged as the backbone of digitization, empowering governments and businesses to navigate dynamic events, unlock new opportunities, and build resilience for swift recovery [1]. Recent global developments underscore the urgency of digital transformation.

Firstly, the three-year pandemic served as a catalyst, accelerating digitization by seven years globally and ten years in Asia Pacific, according to McKinsey [2]. However, corporations now find implementation more challenging, requiring them to act 20-25 times faster than anticipated [2].

Secondly, the global response to climate change is intensifying. The European Union aims for carbon neutrality by 2050, while China pledges to peak emissions by 2030 and achieve neutrality by 2060 [3]. Digital technology presents a key solution, with the World Economic Forum estimating that Information and Communications Technology (ICT) could save 12.1 billion tons of emissions by 2030, ten times its own sector's footprint [4].

Thirdly, the increasingly complex global economic landscape necessitates resilience in business strategies [5]. Digital technology plays a crucial role here, and the low-carbon economy's resurgence further compels businesses to accelerate their digital transformation initiatives.

ISSN 2636-9680
eISSN 2682-9266

Indonesia exemplifies this trend. In the past five years, cloud computing adoption has surged by 48%, significantly exceeding the global average of 19% [6]. A 2021 Thales survey shows that 80% of Indonesian (Small Medium Enterprise) SMEs and large firms utilize cloud solutions in various forms [7]. Reports indicate Indonesia's active embrace of cloud-based technology: 77% of firms already use it, and 83% believe it aids pandemic survival [8]. During the pandemic, 67% of Indonesian enterprises adopted more cloud solutions, while 64% see hybrid cloud solutions as crucial for resilience [8, 9]. Security remains a primary concern, with credential security and solution-infrastructure compatibility being key considerations for 62% of businesses before the pandemic [10].

Cloud computing Indonesia predicts a (Compound Annual Growth Rate) CAGR of 18.9% growth between 2020 and 2024 [11]. By 2021, 50% of SMEs are expected to see a 20% income increase due to cloud adoption, with a projected $10.7 billion boost to Indonesia's GDP over the next five years [11, 12]. The International Data Corporation survey projects Indonesia's public cloud services market to reach US$1.3 billion by 2025, with a 28.1% CAGR from 2020 to 2025 [12].

Despite this progress, challenges remain. Credential security persists as a critical factor for 64% of Indonesian firms during the pandemic, highlighting growing cybersecurity awareness as enterprises expand their digital footprint [13]. A Center for Strategic and International Studies poll reveals that 69.8% of public organizations in Indonesia still do not utilize cloud services due to data security and privacy concerns, with an additional 33.1% citing uncertainties in the rule of law [11].

Cloud computing's adaptability, network-centric approach, and ease of access have driven its popularity among diverse users [14]. However, the immaturity of security technology deters some service providers from fully embracing it, highlighting the need for investment in this area [14]. Additionally, the distributed nature of cloud data, while offering redundancy for disaster recovery, presents potential security risks as data becomes more susceptible to theft and loss [15]. Other security concerns include inadequate user segregation, identity theft, privilege abuse, and insufficient encryption [15].

This study addresses these challenges by conducting a literature review to assess the current state of knowledge surrounding cloud security concerns and potential solutions. We briefly cover the security challenges in cloud computing and explore general strategies that could lead to solutions. Notably, we propose a maturity index for cloud computing security as a key contribution.

The remaining sections of the paper are structured as follows: Section 2 presents related works, Section 3 describes our research methodology, Section 4 focuses on results and discussion, and Section 5 summarizes our findings and provides recommendations in conclusion.

II. RELATED WORK

Cloud security maturity models play a critical role in helping organizations transition to cloud environments securely. These models provide a structured framework for evaluating the effectiveness of security controls, identifying gaps, and implementing best practices to mitigate risks. This literature review explores existing research and publications on cloud security maturity models, focusing on their development, components, application, and impact.

Existing Cloud Security Maturity Models:

- Cloud Security Alliance (CSA) Standards [17]. The CSA advocates a multi-layered approach using virtual LANs, Intrusion Detection/Prevention Systems (IDS/IPS), and firewalls to safeguard data in transit. They also emphasize data leakage prevention due to the shared underlying infrastructure of virtual networks. Additionally, the CSA recommends robust access management solutions.
- Advanced Cloud Protection System (ACPS) Model [18]: This model enhances cloud resource security by offering various services like network protection against user and CSP data breaches. ACPS employs continuous monitoring by the host platform to mitigate cross-tenant attacks. It also enables behavior-based anomaly detection for virtual machines.

- Information Security Management System (ISMS) [19]: ISMS refers to a comprehensive set of policies for managing information security risk. Paper [19] defines it as a standardized approach that addresses all security aspects from a management perspective. It aligns with ISO standards specifying security design, implementation, operation, and management practices.

Information Security (IS) Evaluation:
Information security (IS) evaluation assesses the effectiveness of security controls in protecting organizational information assets. It estimates security risk levels and prioritizes them based on asset value and potential impact. The primary objective is to assess the implemented security controls within an organization. This involves identifying and assessing system risks, measuring security preparedness based on current technology, and comparing results [20, 21].

Securing Cloud Data:
Authors in [22] propose a security approach for cloud-based data using standard and specialized methods with additional recommended measures. Users can assign a 1-10 rating to data secrecy, availability, and integrity needs. These values are used to calculate a "Sensitivity Rating" for the data. Decentralized cloud storage authentication and access control methods have also been explored [23, 24]. Anonymous authentication allows users to verify their identity without revealing it.

Mitigating Post-Violation Risks:
Security breaches or cancellations of Security Service Level Agreements (SLAs) can expose user assets to significant risk. Authors in [25] propose a risk-aware renegotiation approach to mitigate security risks in such situations.

Gaps and Opportunities:
While extensive research addresses security and privacy concerns in cloud computing, much of it focuses on data security, privacy, authorization, and data integrity (Reference 22). We need to explore unlocking the value of reliable data and accelerating digital transformation in terms of sovereignty, economic development, and cybersecurity for both governments and enterprises.

Significant research has been conducted using the KAMI index concept in both public and private sectors. However, further research is needed on constructing a more specific Information Security Maturity Model for cloud security [26]. Existing models like KAMI tend to be broad and limited in scope. To address this, we propose a Cloud Security Maturity Index (CSMI) model that measures the security level of cloud computing services. This approach complements existing assessments conducted by cloud users, as it focuses specifically on cloud provider security practices.

III. METHODOLOGY

The many characteristics of Cloud computing have made the long-dreamed vision of computing as a utility a reality and will potentially shape the whole IT industry. When deciding whether or not to move into the cloud, potential cloud users would consider factors such as service availability, security, and system performance.

Data protection is a crucial security issue for most organizations. Before moving into the cloud, cloud users need to identify data objects to be protected, classify data based on their implication on security, and then follow the security policy for data protection and policy enforcement mechanisms.

The research method used is the literature study method. This strategy emphasizes sifting through journals, papers, and other study materials to locate pertinent information for the issue at hand. This technique examines publications from renowned publishers such as MDPI, IEEE, and Science Direct. All data collected comes from journals, books, or other sources.

Additional resources discovered through exploratory research that are trustworthy, applicable, and fall within the criteria established for this technique are also included. In order for the material or data included in this research study to be accurate and pertinent, a rigorous method or protocol is followed. The

ISSN 2636-9680
eISSN 2682-9266

protocol used in this literature review approach is based on paper [10] recommendations.
The approach is intended for information system researchers who perform most of their study using a literature review technique.

This methodology guarantees the correctness and dependability of data taken from several sources. This method approach can provide knowledge related to cloud security issues and feasible solutions, cloud security, and general tactics that lead to solutions, frameworks for data security governance, and be able to propose maturity indexes for cloud computing security.

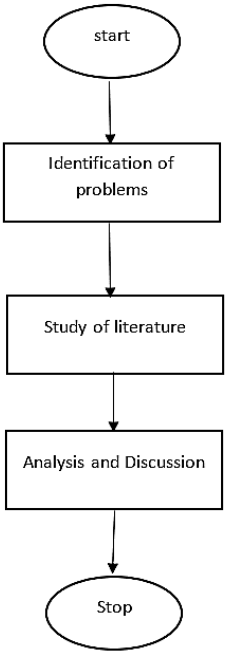

Fig 1. Research Flow

The KAMI Index, developed by the Indonesian government, serves three purposes:

1. **Evaluating Maturity:** It assesses the maturity level of information security management systems (ISMS) within government agencies.
2. **Completeness Assessment:** It measures the completeness of implementation for SNI ISO/IEC 27001:2009, an international standard for ISMS.
3. **Governance Mapping:** It provides a map of the information system security governance landscape within a particular agency.

However, despite its usefulness, the KAMI Index has limitations that necessitate exploring alternative models:

- **Limited Scope:** The KAMI Index primarily offers a basic overview of an agency's information security maturity. It doesn't assess the effectiveness or appropriateness of their ISMS in handling security incidents.
- **Lack of Improvement Guidance:** The Index doesn't provide an improvement plan or recommendations on how to enhance information security practices (protection, maintenance, management, and execution).

These limitations are particularly concerning the recent rise in cyberattacks targeting Indonesia. The escalating cyber threats highlight the critical need for robust information security, a need effectively addressed by well-implemented ISMS.

IV. RESULT & DISCUSSION

This paper proposes a new framework for auditing cloud services, referring to and adopting a framework that categorizes security control activities into three blocks, spanning several domains. CSMI (Cloud Security Maturity Index) is here to assist CSPs in becoming more effective security leaders. It offers a methodical way to evaluate and develop risk management while giving cloud security the respect it merits inside the company.

This framework, called the CSMI (Cloud Security Maturity Index), may be used to level the security dialogue inside your company. It assesses where CSP is now and where the destination is to go. It serves as a guide for CSP to evaluate present and potential partners and vendors. This CSMI framework uses a security domain classification for the cloud model [27], assigning it to each area mentioned in the table below.

TABLE 1: CSMI design domain division

Blocks	Domain
Security	Governance and Enterprise Risk Management
	Security as a Service

Privacy	Data Center Operations
	Information Management and Data Security
	Application Security
	Encryption and Key Management
	Identity and Access Management
	Incident Response, Notification and Remediation
Confidentiality	Legal Issues: Contracts and Electronic Discovery
	Compliance and Audit

The audit process can address one or several domains in a single assessment. An organization must identify its control deficiencies quickly. As such, organizations must understand the effectiveness of their controls and regularly conduct self-audits. Audit findings can help an organization get a complete picture of its compliance and identify deficiencies.

To establish a unified security quality benchmark within an organization, the working group has developed an audit method related to the requirements of the cloud service security (CSS) audit framework.

This CSMI on CSS audit framework may provide detailed security control requirements for CSPs to implement and audit security measures. However, it is not easy to evaluate the effect of these measures beyond their implementation status through audits.

Thus, in addition to auditing, CSPs must measure the impact of their security and privacy protection measures, which requires adequate and feasible cloud security measurement methods and appropriate metrics.

This new framework on measurement of CSS audit framework is mainly done by monitoring and collecting data on key metrics over a while. Organizations can then use the data to analyze and verify changing trends in cloud security across the board. Organizations can understand and evaluate their performance by gathering a sample of metrics.

Regarding NIST SP 800-55r1 and ISO 27004:2016 measurement methods and industry best practices, our new CSS audit framework proposes the following fundamental principles for metric development:

1. Measurable activities: Security management activities must be measurable.
2. Repeatable process: Measurements can be repeated over a certain period.
3. Obtainable data: The established measurement method can obtain adequate data.
4. Comparable results: The data obtained through measurement can be used for comparison and trend analysis.
5. Guidance for management: Analysis of measurement data supports decision-making and helps improve management.

After defining measurement principles, CSPs can design related management metrics and methods following this new framework on cycle measurement and improvement of the CSS audit framework [28]:

One Star: Initial Level: This is the security's first and minimal level of maturity. The CSP has implemented the security controls defined by ISO/IEC 27001 on a basic level, which provides a management framework for implementing an information security management system (ISMS). The security management processes and tools are not developed systematically but are implemented based on practices.

• Two Stars: Basic Level: To have compliance with the two-star security assurance of CSMI, some more security-specific tools/techniques will be required to be adopted by the organizations for more secure software development. The CSP's security controls cover most controls defined in level-1 basic requirements of the new KAMI regarding the CSS audit framework. The CSP has developed and maintained formal processes and provided related tools.

• Three Stars: Intermediate Level: At this level, security must be planned and implemented very preciously in all the processes at every stage of the development life cycle. The CSP complies with the review and measurement methods defined by the new framework regarding the CSS audit framework and conducts regular assessments and improvements of cloud security governance capabilities.

• Four Stars: Advanced Level: This is an advanced level of security. The CSP widely uses mature management technologies and tools and has industry-leading capabilities in

ISSN 2636-9680
eISSN 2682-9266

certain key business domains. The cloud security governance system is constantly monitored, measured, evaluated, and optimized.

• Five Stars: Leading Level: This is the final and five stars level in which the development organization will offer the software with maximum achievable security. The CSP widely uses mature security management technologies and tools and can develop innovative solutions. The CSP has developed innovative security governance methodologies.

TABLE 2: Maturity Level and Description

Maturity Level and Description	
Initial	• The CSP has established a security management system based on widely accepted industry standards (such as ISO/IEC 27001) and provided basic security management capabilities. • The CSP has implemented the security controls defined by ISO/IEC 27001 on a basic level, which provides a management framework for implementing an information security management system (• The security management processes and tools are not developed in a systematical manner but are implemented based on practices. • Basic information security management documents are in place.
Basic	• The CSP has established a cloud service cyber security and compliance governance system based on the 3CS framework. • The CSP's security controls cover most controls defined in level-1 basic requirements of the new KAMI regarding cloud service security audit framework. • The CSP has developed and maintained formal processes and provided related tools. • The CSP has released formal management documents and conducted regular maintenance through formal processes.
Intermediate	• The CSP has the capability to meet most level-2 basic requirements defined by the new KAMI regarding cloud service security audit framework and has provided certain process automation supported by mature tools. • The CSP complies with the review and measurement methods defined by the new KAMI regarding on cloud service security audit framework and conducts regular assessment and improvement of cloud security governance capabilities.
Advanced	• The CSP has the capabilities to meet most level-2 basic requirements defined by the new KAMI regarding on cloud service security audit framework and meet most level-2 supplementary requirements. • The CSP widely uses mature management technologies and tools and has industry-leading capabilities in certain key business domains. • The cloud security governance system is constantly monitored, measured, evaluated, and optimized.
Leading	• The CSP has the capabilities to meet all level-2 basic requirements defined in the new KAMI regarding on cloud service security audit framework as well as all level-2 supplementary requirements. • The CSP widely uses mature security management technologies and tools and is able to develop innovative solutions. • The CSP has developed innovative security governance methodologies.

V. CONCLUSION

This research, informed by both literature and web searches, explores the advantages, disadvantages, and challenges associated with a country's transition to cloud computing. One potential drawback lies in vendor lock-in, where contract termination fees can create revenue losses.

This research emphasizes the importance of robust cloud security for countries choosing suitable cloud service providers aligned with their goals. Cloud technology can foster innovation and knowledge creation, but vendor lock-in presents a significant concern.

As a new technology adopted by countries for market growth, cloud security is paramount due to the storage of sensitive data. Fortunately, cloud security systems effectively encrypt and verify transmitted information before decryption.
This paper examines existing security standards used by the Indonesian government to enhance security and raise awareness of national vulnerabilities.

While offering valuable findings, the paper recognizes several limitations:

1. Context-Specific Adaptability: While acknowledging the importance of context in cloud security maturity models, the paper lacks a detailed exploration and implementation of this concept. Future research could delve deeper into the impact of organizational context (industry, size, deployment model) on maturity model design and application.

2. Validation and Empirical Testing: The proposed cloud security maturity index lacks extensive empirical validation in real-world settings. Future research could conduct case studies and empirical studies to assess the effectiveness and applicability of such models across diverse contexts, providing valuable insights into their practical utility and limitations.

3. User-Centric Perspectives: While user perspectives are briefly mentioned, the paper lacks in-depth exploration of user-centric aspects like usability, user experience, and organizational culture. Future research could incorporate user-centric design principles into maturity models to enhance usability and adoption, considering the diverse needs and preferences of stakeholders involved in cloud security management.

Effective cloud security can significantly impact state-owned programs. Future research could explore relevant regulations and laws, as well as the impact of cloud computing on national organizational structures.

In conclusion, the cloud security provided will be able to impact the programs owned by the state. In the future, further research can be carried out regarding the regulations and laws that must be complied with by cloud security; and, how the cloud affects the organizational structure of countries.

VI. REFERENCES

[1] M. Hamad, A. Kuwaiti, and T. M. al Kaissi, "A Comprehensive Reconsideration of Cloud Security Approach," *OIC-CERT Journal of Cyber Security*, vol. 4, no. 1, p. 51, 2022.

[2] McKinsey, "Capture a digital transformation's value today," 2022. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/three-new-mandates-for-capturing-a-digital-transformations-full-value (accessed Jan. 28, 2023).

[3] P. Friedlingstein *et al.*, "Global carbon budget 2019," *Earth Syst Sci Data*, vol. 11, no. 4, pp. 1783–1838, Dec. 2019, doi: 10.5194/ESSD-11-1783-2019.

[4] S. Panchiwala and M. Shah, "A Comprehensive Study on Critical Security Issues and Challenges of the IoT World," *Journal of Data, Information and Management*, vol. 2, no. 4, pp. 257–278, Dec. 2020, doi: 10.1007/S42488-020-00030-2.

[5] D. Angamuthu and N. Pandian, "A Study of the Cloud Computing Adoption Issues and Challenges," *Recent Advances in Computer Science and Communications*, vol. 13, no. 3, pp. 313–318, Aug. 2020, doi: 10.2174/2213275911666181114142428.

[6] F. D. Mobo, "Cloud Computing Security, Privacy and Forensics: Issues and Challenges Ahead," *International Journal of Recent Trends in Engineering and Research*, vol. 4, no. 3, pp. 10–13, Mar. 2018, doi: 10.23883/IJRTER.2018.4083.XWPNA.

[7] Thales, "The Challenges of Data Protection in a Multicloud World," 2022.

[8] L. Vishwakarma, R. Shukla, and S. Pavani, "SECURITY RELATED ISSUES AND CHALLENGES IN CLOUD ENVIRONMENT," *Wutan Huatan Jisuan Jishu*, vol. 17, no. 7, 2021, Accessed: Jan. 28, 2023. [Online]. Available: https://cmdpgcollege.ac.in/Uploads/SECURITY%20RELATED%20ISSUES%20AND%20CHALLENGES%20IN%20CLOUD_2021037080626.pdf

[9] S. Panchiwala, M. S.-J. of Data, I. and Management, and undefined 2020, "A comprehensive study on critical security issues and challenges of the IoT world," *Springer*, Accessed: Jan. 28, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s42488-020-00030-2

ISSN 2636-9680
eISSN 2682-9266

[10] A. S. AlAhmad, H. Kahtan, Y. I. Alzoubi, O. Ali, and A. Jaradat, "Mobile cloud computing models security issues: A systematic review," *Journal of Network and Computer Applications*, vol. 190, p. 103152, Sep. 2021, doi: 10.1016/j.jnca.2021.103152.

[11] A. Gui, Y. Fernando, M. S. Shaharudin, M. Mokhtar, I. G. M. Karmawan, and - Suryanto, "Cloud Computing Adoption Using TOE Framework for Indonesia's Micro Small Medium Enterprises," *JOIV : International Journal on Informatics Visualization*, vol. 4, no. 4, p. 237, Dec. 2020, doi: 10.30630/joiv.4.4.458.

[12] L. Sanny, A. Hamada, A. Prameswari, and A. Setiawan, "Effects of Social Media Marketing in Cloud Kitchen Towards Online Platform in Indonesia," in *2022 International Seminar on Application for Technology of Information and Communication (iSemantic)*, Sep. 2022, pp. 367–371. doi: 10.1109/iSemantic55962. 2022.9920470.

[13] A Bayunata, "Analysis Of Minimum Design Security For Private Cloud In Indonesia Using NIST Sp 800-30 To Fulfill ISO 27001," *Master of Information Technology*, 2023, Accessed: Jan. 28, 2023. [Online]. Available: https://thesis.sgu.ac.id/ index.php/ots/article/view/3994

[14] D. Moh. and W. Millary Agung, "Utilization EOS Platform as cloud-based GIS to analyze vegetation greenness in Cirebon Regency, Indonesia," *Journal Of Information Technology And Its Utilization*, vol. 3, no. 1, pp. 1–4, 2020, Accessed: Jan. 28, 2023. [Online]. Available: http://karya.brin.go.id/id/eprint/13806/

[15] F. Murni, M. Heikal, A. Suhaimi, and M. Khaleel, "Intention to adopt cloud accounting: A conceptual model from Indonesian MSMEs perspectives," *koreascience.or.kr*, vol. 7, no. 12, pp. 749–759, 2020, doi: 10.13106/jafeb .2020.vol7.no12.749.

[16] N. Santoso, A. Kusyanti, H. Puspa, and Y. April, "Trust and Security Concerns of Cloud Storage: An Indonesian Technology Acceptance," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 6, pp. 453–458, 2018, doi: 10.14569/IJACSA.2018.090662.

[17] Cloud Security Alliance, "Cloud Security Alliance's Top Threats to Cloud," Jun. 07, 2022. https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning/ (accessed Jan. 29, 2023).

[18] F. Lombardi and R. di Pietro, "Secure virtualization for cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1113–1122, Jul. 2011, doi: 10.1016/j.jnca.2010.06.008.

[19] H. Hambali and P. Musa, "Analysis Of Governance Security Management Information System Using Index Kami In Central Government Institution," *Angkasa: Jurnal Ilmiah Bidang Teknologi*, vol. 12, no. 1, Mar. 2020, doi: 10.28989/angkasa.v12i1.563.

[20] Y. Fernando, S. Achmad, and A. Gui, "Leveraging business competitiveness by adopting cloud computing in Indonesian creative industries," *Int J Bus Inf Syst*, vol. 32, no. 3, pp. 364–392, 2019, doi: 10.1504/IJBIS.2019.103082.

[21] M. N. Sahid Ramadhan, A. Amyus, A. N. Fajar, S. Sfenrianto, A. F. Kanz, and M. S. Mufaqih, "Blood Bank Information System Based on Cloud Computing In Indonesia," *J Phys Conf Ser*, vol. 1179, no. 1, p. 012028, Jul. 2019, doi: 10.1088/1742-6596/1179/1/012028.

[22] 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, doi: 10.1109/ACCESS.2020.2985762.

[23] C. J. Vijaya, C. Narasimham, and P. Sai Kiran, "Authentication and Authorization Mechanism for Cloud Security," *Int J Eng Adv Technol*, vol. 8, no. 6, pp. 2072–2078, Aug. 2019, doi: 10.35940/ijeat. F8473.088619.

[24] T. Alam, "Cloud Computing and its role in Information Technology," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 1, no. 2, pp. 108–115, Feb. 2020, doi: 10.34306/itsdi.v1i2.103.

[25] S. Feng, Z. Xiong, D. Niyato, P. Wang, S. S. Wang, and S. X. Shen, "Joint Pricing and Security Investment in Cloud Security Service Market with User Interdependency," *IEEE Trans Serv Comput*, vol. 15, no. 3, pp. 1461–1472, May 2022, doi: 10.1109/TSC.2020.2996382.

[26] N. B. Muhammad and M. Bazzi, "Advances in Cloud Computing: Security Issues and Challenges in the Cloud," in *2022 5th International Conference on Information and Computer Technologies (ICICT)*, Mar. 2022, pp. 110–116. doi: 10.1109/ ICICT55905.2022.00027.

[27] G. Mateescu and M. Vlădescu, "Auditing Hybrid IT Environments," 2014. [Online]. Available: www.ijacsa.thesai.org

[28] S. K. Pandey, "Security Vigilance System through Level Driven Security Maturity Model," *International Journal of Computer Science, Engineering and Information Technology*, vol. 2, no. 2, pp. 11–17, Apr. 2012, doi: 10.5121/ijcseit.2012.2202.

ISSN 2636-9680
eISSN 2682-9266