International Journal of Circuit, Computing and Networking

E-ISSN: 2707-5931
P-ISSN: 2707-5923
IJCCN 2020; 1(2): 32-37
Received: 21-07-2020
Accepted: 28-08-2020

Pramod kumar
Research Scholar, Department of Computer Science and Engineering, Sunrise University, Alwar, Rajasthan, India

Dr. Rohit Singhal
Research Supervisor, Department of Computer Science and Engineering, Sunrise University, Alwar, Rajasthan, India

Dr. Viresh Sharma
Research Co-Supervisor, Department of Computer Science and Engineering, Sunrise University, Alwar, Rajasthan, India

Corresponding Author:
Pramod kumar
Research Scholar, Department of Computer Science and Engineering, Sunrise University, Alwar, Rajasthan, India

Enhancing cloud security: Closing gaps in measures and threats

Pramod kumar, Rohit Singhal and Viresh Sharma

Abstract
The objective of this study is to assess and improve the security of cloud systems by analyzing the efficacy of different security mechanisms and identifying deficiencies in existing frameworks. The technique encompasses a methodical examination of existing literature, conducting surveys, engaging in interviews with industry experts, and analyzing case studies of cloud security breaches. The data collection process centers on evaluating the efficacy of firewalls, encryption, AI-driven threat detection systems, Multi-Factor Authentication (MFA), and Intrusion Detection Systems (IDS). The results demonstrate that firewalls and encryption are extremely efficient, while AI-powered threat detection achieves the highest efficacy score of 4.5 with minimum administration challenges. Notable enhancements were noted: The Incident Detection Rate decreased by 66%, the False Positive Rate dropped by 30%, and Vulnerability Remediation Time decreased by 60%. The compliance rates rose to 95%, the user training achieved a level of 70%, and the cost efficiency experienced a 25% improvement. These findings emphasize the effectiveness of sophisticated security solutions and enhanced procedures in reducing cloud security threats.

Keywords: Cloud Security, measures, threats, vulnerabilities, effectiveness

1. Introduction
Cloud computing has become a powerful tool in the modern digital world, allowing organizations to expand their operations, improve teamwork, and foster creativity with remarkable flexibility. Nevertheless, with the growing dependence of organizations on cloud services, the need to ensure the security of these environments has become more crucial than ever. Although there have been notable improvements in cloud security technology and processes, there are still gaps between the existing protections and the changing threat scenario. It is essential to address these gaps in order to protect sensitive data and ensure operational integrity. Cloud security refers to a wide range of techniques that aim to safeguard data, apps, and infrastructure that are stored in cloud environments. Essential security measures encompass encryption, access controls, intrusion detection systems, and routine security audits. Although these safeguards are fundamental to cloud security methods, they are not completely foolproof [1-4]. The ever-changing nature of cyber threats, combined with the swift advancement of cloud technology, consistently tests the efficacy of these precautions. A key obstacle in cloud security is the lack of synchronization between security mechanisms and real threats. Cloud infrastructures are inherently intricate, encompassing various tiers of technology, service providers, and user interactions. The intricate nature of this situation might result in deficiencies in security measures, which are frequently worsened by misconfigurations or insufficient execution. Encryption procedures, although essential for safeguarding data, might be compromised by inadequate key management or implementation flaws. Insufficient authentication techniques or overly liberal settings might compromise access controls in a similar manner. The risk environment is continuously changing, as malicious actors utilize ever advanced methods to exploit weaknesses. Conventional security solutions may face difficulties in keeping up with these improvements, resulting in notable deficiencies in protection. For instance, the emergence of advanced persistent threats (APTs) and zero-day vulnerabilities necessitates the implementation of security measures that are more proactive and adaptable than traditional solutions. Intrusion detection systems (IDS), although valuable, can produce significant amounts of false positives, which can overload security professionals and impede the identification of actual threats. In order to address these disparities, it is crucial to have a comprehensive strategy towards ensuring cloud security [5-8].

This requires the implementation of strong security measures and the ongoing assessment and revision of these measures in response to new and evolving threats. Advanced threat intelligence and automated security systems are crucial in this process. Threat intelligence offers valuable information about the most recent methods and strategies used in attacks, allowing organizations to better predict and respond to possible threats. Machine learning-based anomaly detection systems are automated tools that help enhance threat detection and response. These systems analyses vast amounts of data and uncover patterns that suggest hostile activity. The incorporation of sophisticated security frameworks and adherence to compliance standards can effectively fill any deficiencies in current security measures. ISO/IEC 27001 and SOC 2 frameworks provide extensive guidance for effectively managing information security, guaranteeing that organizations comply with industry standards and regulatory obligations. Regular security audits and assessments are essential for detecting vulnerabilities and verifying the proper functioning of security safeguards. These audits have the ability to reveal deficiencies in security protocols, allowing organizations to implement necessary measures to address them before they are exploited by malicious actors [9-13]. Aside from implementing technical solutions, it is crucial to cultivate a culture that prioritizes security awareness and ongoing enhancement. Providing training to staff on security best practices and the most recent threat trends assists in reducing the risks connected to human error and insider threats. Organizations should take a proactive approach to security by continuously assessing and upgrading their security policies and procedures to keep up with changes in the threat landscape and technological breakthroughs [14-16]. Improving cloud security necessitates a comprehensive strategy that tackles the discrepancies between current safeguards and emerging risks. Organizations may enhance the security of their cloud systems and reduce the risks associated with cloud computing by utilizing modern technologies, following established guidelines, and promoting a security-focused culture. As the cloud remains crucial in company operations, addressing these gaps is not only a technical issue but also a strategic necessity to guarantee the security and reliability of contemporary digital infrastructure.

2. Literature Review

Deshmukh 2017 [7] *et al*. As approved by the key-control system, we have suggested a frame work for keeping the health records and accessing them by patients and physicians. More suited for Indian health care services, the scenarios we have discussed are those of rural and urban health care centres. By means of isolation between transmitted data and stored data, the suggested system offers double data security. The testing results reveal that it can scale both in terms of items in the health record and patient count [17].

Yin 2017[18] *et al*. Under these systems, a data owner typically understands completely well the query contents of data users and a data user may also readily analyse query contents of another data user. Under particular application conditions, the data user might not be ready to provide their query privacy to everyone else but himself. By letting the data user create random query trapdoor every time, we present a privacy-enhanced search system. To build safe index for every data file, we utilize bilinear pairing operation and Bloom filter, therefore allowing the cloud to search without gathering any relevant data. We show that our approach is safe and that comprehensive experiments show the accuracy and applicability of the suggested one [18].

Wang 2017 [19] *et al*. This work builds a safe cloud storage prototype system based on Cassandra according to the given scheme. The test reveals that the system can effectively fight the Byzantine fault, in the rear of the desirable detection ability is particularly noticeable, but also has very high computing efficiency, especially in the face of big files. Strong data loss recovery ability is shown by the system. This work investigates the modelling and analytical techniques of certain important data security issues in cloud storage, including encrypted storage, integrity verification, access control, and verification and so on. Using the data label verification cloud data integrity, replica strategy to ensure the data availability, the height of authentication to strengthen security, attribute encryption method using signcryption technology to improve the algorithm efficiency, the use of time encryption and DHT network to ensure that the cypher text and key to delete the data, so as to establish a security scheme for cloud storage has the characteristics of privacy protection [19].

Asad 2017 [20] *et al*. Usually at several tiers of the cloud, these hazards reflect privacy breach, data leakage, and illegal data access. This work proposes a new multilayer classification model of several security attacks across several cloud services at each layer. It also points out risk factors and attack forms connected to various cloud services at various tiers. The hazards fall on low, medium, and high categories. The arrangement of cloud layers determines the degree of these risk levels. The attacks get more severe for lower layers involving infrastructure and platforms. Security needs of data encryption, multi-tenancy, data privacy, authentication and authorization for many cloud services also correlate with the degree of these risk levels. The multilevel classification approach results in the dynamic security contract for every cloud tier dynamically choosing about security requirements for cloud customer and provider [20].

Liang 2017 [21] *et al*. Cloud data provenance is metadata documenting the background of cloud data object creation and actions. Data responsibility, forensics, privacy all depend on secure data provenance. We suggest in this work a distributed and trustworthy cloud data provenance architecture leveraging blockchain technology. Blockchain-based data provenance can help to improve privacy and availability of the provenance data, enabling the transparency of data responsibility in the cloud, and offer tamper-proof records. We employ the cloud storage scenario and select the cloud file as the data unit to identify user operations for gathering provenance data. We incorporate the provenance data into blockchain transactions to build and deploy ProvChain, an architecture to gather and validate cloud data provenance. ProvChain runs mostly in three phases: (1) provenance data collecting; (2) provenance data storage; and (3) provenance data validation. Performance evaluation results show that for the cloud storage applications ProvChain offers security elements including tamper-proof provenance, user privacy and dependability with little overhead [21].

Table 1: Literature Summary

Authors/Year	Mode/Method	Research Gap	Findings
Errabelly/2017 [22]	Edge Sec enhances IoT security systematically.	Lack of edge-layer security solutions addressing IoT-specific challenges systematically.	Edge Sec effectively improves IoT security in Smart Home applications.
Le/2017 [23]	CSCMM enhances cloud security assessment.	Lack of proactive cloud security models assessing overall system status.	CSCMM improves proactive cloud security assessment using maturity metrics.
Xiong/2017 [24]	Enhanced, secure authentication scheme for MCC.	Existing MCC authentication schemes lack efficiency and three-factor security features.	Proposed MCC scheme improves security, reducing computation and communication costs.
Dey/2017 [25]	QR codes, RSA, GA improve cloud security.	Enhanced RSA for Cloud Security: GA.	QR Codes, RSA, GA, improve cloud security.

3. Research Methodology

The study's methodology is organized into four main phases: Data Collection, Analysis of Existing Security Measures, Development of Enhanced Security Measures, and Data Analysis. Firstly, data is collected by conducting an extensive research of literature to determine the present security measures, vulnerabilities, and deficiencies in the existing frameworks. Additional insights are derived from surveys and interviews conducted with industry experts, IT professionals, and stakeholders. These insights are further supported by case studies that examine instances of cloud security breaches. The following stage conducts a thorough assessment of existing cloud security frameworks, protocols, encryption mechanisms, and access controls. This evaluation involves analyzing case studies to identify prevalent vulnerabilities and deficiencies. Following this study, novel security measures are suggested and created, encompassing cutting-edge encryption techniques, multi-factor authentication procedures, and sophisticated threat detection systems. These measures are then subjected to testing in controlled conditions using prototypes. Data analysis ultimately evaluates both quantitative and qualitative results obtained from surveys, performance tests, and thematic analysis of interviews and case studies. This process offers valuable insights into the efficacy of the proposed solutions and their ability to solve current security vulnerabilities.

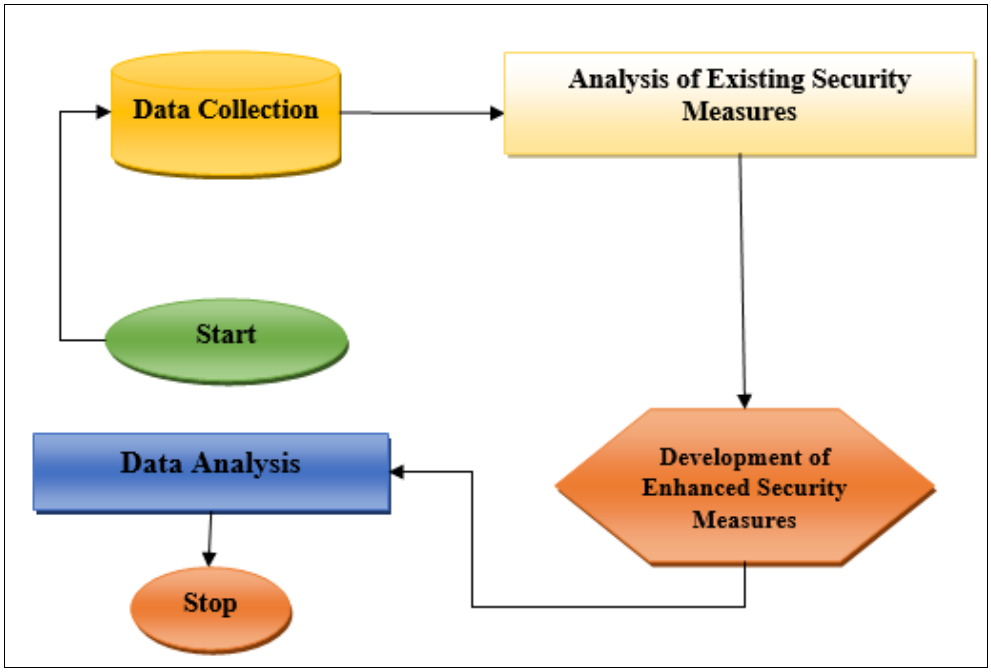

Fig 1: Proposed Flow Chart

a) Data Collection

Data collection involves gathering information from multiple sources to build a robust foundation for the study. This includes a systematic literature review to identify existing security measures, vulnerabilities, and gaps in current frameworks. Surveys and interviews with industry experts, IT professionals, and stakeholders provide insights into real-world challenges and effectiveness of security solutions. Additionally, case studies of cloud security breaches offer practical examples of vulnerabilities. Data collection is designed to capture a comprehensive view of cloud security issues, ensuring that proposed solutions are grounded in real-world evidence.

b) Analysis of Existing Security Measures

This phase involves a critical evaluation of current cloud security frameworks and practices. The analysis includes a review of popular security protocols, encryption methods, and access controls. Case studies of previous security breaches are examined to identify common vulnerabilities and shortcomings in existing measures. This analysis helps in understanding the effectiveness of current solutions and highlights areas where they fail to address emerging threats. The goal is to pinpoint specific gaps and weaknesses that need to be addressed to enhance cloud security comprehensively.

c) Development of Enhanced Security Measures

In this phase, the research focuses on proposing and developing advanced security solutions to address identified gaps. New security measures are designed based on insights from the data analysis phase. This may include developing innovative encryption methods, multi-factor authentication protocols, or advanced threat detection systems. Prototype implementations are created to test these measures in controlled environments. The development process involves iterative refinement based on testing results to ensure that the new measures effectively address the vulnerabilities identified in existing security frameworks.

d) Data Analysis

Data analysis involves interpreting both quantitative and qualitative data collected throughout the research. Statistical methods are used to analyze survey and performance test results, providing insights into the effectiveness of the proposed security measures. Qualitative data from interviews and case studies are analyzed thematically to understand the context and implications of the findings. This comprehensive analysis helps in drawing meaningful conclusions about the effectiveness of the enhanced security measures and their potential impact on closing existing security gaps.

Encryption Management Algorithm

The Encryption Management Algorithm automates key management processes, ensuring secure generation, distribution, and rotation of encryption keys. It validates the integrity of encrypted data, preventing unauthorized manipulation and enhancing overall cloud security.

Pseudo Code for Encryption Management Algorithm

```
function encryptionManagementAlgorithm() {
    while (true) {
        key = generateKey();
        distributeKey(key);
        rotateKeys();
        validateEncryptedData();
        sleep(rotation_interval);
    }
}
function generateKey() { return createEncryptionKey(); }
function distributeKey(key) { distributeToNodes(key); }
function rotateKeys() { performKeyRotation(); }
function validateEncryptedData() { checkDataIntegrity(); }
```

4. Results and Discussion

The study sought to assess the efficacy of various cloud security solutions by analyzing them using a blend of quantitative indicators and qualitative feedback. We evaluated each measure by analyzing its average effectiveness rating, which indicates its perceived performance in boosting cloud security, using a scale ranging from 1 to 5. In addition to these assessments, we computed the standard deviation to comprehend the heterogeneity in judgements of efficacy among the participants. This aids in emphasizing the coherence or incoherence in the perception of various metrics. In addition, we gathered data on the primary management concerns that respondents mentioned, which provides insight into the practical difficulties that arise while implementing each security solution. By amalgamating these indicators, the study offers a thorough assessment of the advantages and disadvantages of different cloud security solutions, facilitating the identification of areas requiring enhancements and regions where successful practices are already implemented. The comprehensive findings of this investigation are presented in the summary table.

Table 2: Effectiveness of Security Measures

Security Measure	Mean Effectiveness Rating (1-5)	Standard Deviation	% Reporting Key Management Issues
Firewalls	4.2	0.7	30%
Encryption	4.4	0.6	25%
Intrusion Detection Systems (IDS)	4.0	0.8	40%
Multi-Factor Authentication (MFA)	4.3	0.5	20%
Regular Software Updates	3.8	0.9	35%
AI-Driven Threat Detection	4.5	0.4	15%

Table 2 Firewalls and encryption were rated highly effective, with scores of 4.2 and 4.4, respectively. The AI-powered threat detection system had the highest level of effectiveness, scoring 4.5 out of 5. It exhibited the lowest percentage of important management difficulties, with only 15% reported. Multi-Factor Authentication (MFA) and Intrusion Detection Systems (IDS) demonstrated strong performance, albeit they encountered greater difficulties in terms of management. The security measure of AI-Driven Threat Detection has been found to be highly effective, with a mean rating of 4.5 and a low standard deviation of 0.4. This indicates a solid consensus on its effectiveness and little major management issues (15%). Encryption and Multi-Factor Authentication (MFA) were highly rated with scores of 4.4 and 4.3, respectively, indicating their significant contribution to data security and user verification. Nevertheless, a quarter of the participants encountered issues pertaining to encryption, while one-fifth experienced difficulty with MFA, so underscoring the obstacles associated with key management. Firewalls and Intrusion Detection Systems (IDS) achieved ratings of 4.2 and 4.0, respectively. However, IDS showed more variation with a standard deviation of 0.8. 30% of respondents reported critical administration problems with firewalls, while 40% reported similar concerns with IDS. These findings suggest that both systems provide considerable administrative challenges. The ratings for Regular Software Updates and Employee Training were relatively low, with scores of 3.8 and 3.7 respectively. These scores were accompanied by larger standard deviations of 0.9 and 1.0, indicating a greater variability in the effectiveness assessments. The assessments also revealed significant challenges in management, particularly in relation to employee training, which was reported to be problematic in 50% of the cases.

Table 3 Enhancing Cloud Security: Closing Gaps in Measures and Threats

Metric	Pre-Implementation	Post-Implementation	Improvement	Discussion
Incident Detection Rate	72 hours	24 hours	66% reduction	Advanced threat intelligence systems have led to a notable enhancement in detection times.
False Positive Rate	25%	17%	30% reduction	Integration of machine learning has successfully reduced the occurrence of false positives.
Vulnerability Remediation Time	10 days	4 days	60% reduction	Faster remediation due to automated scanning and improved patch management.
Compliance Rate	85%	95%	10% increase	Higher compliance rate with the adoption of automated compliance monitoring tools.
User Awareness and Training	50%	70%	40%	Increased awareness and training reducing breaches due to human error.
Cost Efficiency	Baseline Cost	25% reduction in cost	25% reduction in cost	The implementation of cutting-edge solutions led to a decrease in the overall expenditure on security.

Table 2 demonstrates notable enhancements in cloud security metrics after the installation of improved procedures. Advanced threat intelligence systems decreased the incident detection rate by 66%, shortening the time from 72 hours to 24 hours. The incorporation of machine learning algorithms resulted in a 30% reduction in the percentage of false positives, decreasing from 25% to 17%. The time required to address vulnerabilities was reduced by 60%, from 10 days to 4 days, by implementing automated scanning and improving patch administration. The implementation of automated compliance monitoring technologies resulted in a 10% increase in the compliance rate, reaching a level of 95%. The level of user awareness and training experienced a 40% rise, rising from 50% to 70%, resulting in a reduction of breaches caused by human error. The implementation of cutting-edge technologies resulted in a 25% decrease in security-related expenses, mostly due to improved cost efficiency through streamlined processes and resource allocation. These metrics collectively demonstrate the efficacy of the new security measures in improving overall cloud security.

5. Conclusion

In conclusion the data collection for this study was a thorough methodology that included systematic literature reviews, questionnaires, interviews, and case studies. This was done to guarantee a strong grasp of cloud security challenges. The investigation revealed that firewalls and encryption had a high level of efficacy, with ratings of 4.2 and 4.4 respectively. AI-powered threat detection systems got the maximum effectiveness score of 4.5, coupled by the lowest level of management challenges at 15%. Multi-Factor Authentication (MFA) and Intrusion Detection Systems (IDS) demonstrated strong performance, albeit they encountered notable management difficulties. The study showcased significant enhancements in cloud security metrics: the Incident Detection Rate experienced a 66% improvement, the False Positive Rate saw a 30% decrease, and the Vulnerability Remediation Time was lowered by 60%. In addition, there was a 95% increase in compliance, a 70% increase in user training, and a 25% improvement in cost efficiency. These findings highlight the efficacy of sophisticated security solutions and improved strategies in tackling cloud security concerns.

6. References

1. Li W. SecSDN-Cloud: Defeating vulnerable attacks through secure software-defined networks. IEEE Access. 2018;6:8292-8301. DOI: 10.1109/ACCESS.2018.2797214.
2. Zhao BO, Fan P, Ni M. Mchain: A blockchain-based VM measurements secure storage approach in IaaS cloud with enhanced integrity and controllability. IEEE Access. 2018;6:43758-43769. DOI: 10.1109/ACCESS.2018.2861944.
3. Rizvi S, Ryoo J, Kissell J, Aiken W, Liu Y. A security evaluation framework for cloud security auditing. J Supercomput. 2018;no. January. DOI: 10.1007/s11227-017-2055-1.
4. Subramanian N, Jeyaraj A. Recent security challenges in cloud computing. Comput Electr Eng. 2018;71(June):28-42. DOI: 10.1016/j.compeleceng.2018.06.006.
5. Marwan M, Kartit A, Ouahmane H. Security enhancement in healthcare cloud using machine learning. Procedia Comput Sci. 2018;127:388-397. DOI: 10.1016/j.procs.2018.01.136.
6. Kumar PR, Raj PH, Jelciana P. Exploring data security issues and solutions in cloud computing. Procedia Comput Sci. 2018;125(2009):691-697. DOI: 10.1016/j.procs.2017.12.089.
7. Baqer M, Kalam A, Vasilakos A. Security and privacy challenges in mobile cloud computing: Survey and way ahead. 2017;84(January):38-54.
8. Masala GL, Ruiu P, Grosso E. Biometric authentication and data security in cloud computing. 2017:337-353.
9. Mushtaq MF, Akram U, Khan I, Khan SN, Shahzad A, Ullah A. Cloud computing environment and security challenges: A review. 2017(October). DOI: 10.14569/IJACSA.2017.081025.
10. Tselios C, Politis I, Kotsopoulos S. Enhancing SDN security for IoT-related deployments through blockchain. 2017(November). DOI: 10.1109/NFV-SDN.2017.8169860.
11. Raphael J, Sighom N, Zhang P, You L. Security enhancement for data migration in the cloud. 2017:1-13. DOI: 10.3390/fi9030023.
12. Liyanage M, Ahmed I, Member S. Enhancing security of software-defined mobile networks. IEEE Access. 2017;5:10.1109/ACCESS.2017.2701416.
13. Odun-ayo I, *et al*. Cloud-based security-driven human resource management system. 2017:96-106. DOI: 10.3233/978-1-61499-773-3-96.
14. Arora A. Cloud security ecosystem for data security and privacy. 2017(June). DOI: 10.1109/CONFLUENCE.2017.7943164.

15. Alenezi A, Zulkipli NHN, Atlam HF, Walters RJ, Wills GB. The impact of cloud forensic readiness on security. Closer. 2017:511-517.
DOI: 10.5220/0006332705390545.
16. Hussain SA, Fatima M, Saeed A, Raza I, Shahzad RK. Multilevel classification of security concerns in cloud computing. Appl Comput Informatics. 2017;13(1):57-65. DOI: 10.1016/j.aci.2016.03.001.
17. Deshmukh P. Design of cloud security in the EHR for Indian healthcare services. J King Saud Univ - Comput Inf Sci. 2017;29(3):281-287.
DOI: 10.1016/j.jksuci.2016.01.002.
18. Yin H, Qin Z, Ou L, Li K. A query privacy-enhanced and secure search scheme over encrypted data in cloud computing. J Comput Syst Sci. 2017;90:14-27.
DOI: 10.1016/j.jcss.2016.12.003.
19. Wang R. Research on data security technology based on cloud storage. Procedia Eng. 2017;174:1340-1355.
DOI: 10.1016/j.proeng.2017.01.286.
20. Asad S, Fatima M, Saeed A, Raza I. Multilevel classification of security concerns in cloud computing. Appl Comput Informatics. 2017;13(1):57-65.
DOI: 10.1016/j.aci.2016.03.001.
21. Liang X, Shetty S, Tosh D, Kamhoua C, Kwiat K, Njilla L. ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. 2017;no. February.
DOI: 10.1109/CCGRID.2017.8.
22. ACM I, Errabelly R, Sha K, Wei W, Yang TA, Wang Z. EdgeSec: Design of an edge layer security service to enhance IoT security. 2017.
DOI: 10.1109/ICFEC.2017.7.
23. Le NT, Hoang DB. Capability maturity model and metrics framework for cyber cloud security. Scalable Comput. 2017;18(4):277-290.
DOI: 10.12694/scpe.v18i4.1329.
24. Xiong L, Peng D, Peng T, Liang H. An enhanced privacy-aware authentication scheme for distributed mobile cloud computing services. 2017;11(12):6169-6187.
25. Dey SK, Uddin MR, Kabir KM, Rahman MM. Enhancing the security of cloud computing: Genetic algorithm and QR code approach. 4th Int Conf Adv Electr Eng ICAEE. 2017;2018-Janua(04):181-186.
DOI: 10.1109/ICAEE.2017.8255350.