International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT12390146

Improving Security for the Users Data by using Security Certification System in Cloud Computing

K V V Satya Trinadh Naidu[1], V. Sravani Kumari[2], Dr. Mahesh Kotha[3], M Mounika[4], Dr. G Vinoda Reddy[5]

[1]Assistant Professor, CSE(AI) Department, Madanapalle institute of Technology & Science, Madanapalle.

[2]Assistant Professor, Department of CSE(DS), CMR Engineering College, Hyderabad, India

[3]Associate professor, Department of CSE (AI&ML), CMR Technical Campus, Hyderabad, India

[4]Assistant Professor, Department of CSE(DS), TKR College of Engineering and Technology, Hyderabad, India

[5]Professor, CSE (AI & ML) Department, CMR Technical Campus, Hyderabad, India

ARTICLEINFO

Article History:

Accepted: 01 July 2023

Published: 15 July 2023

Publication Issue

Volume 9, Issue 4

July-August-2023

Page Number

114-123

ABSTRACT

Cloud computing has emerged as a dominant paradigm in the field of information technology, offering a flexible and scalable platform for storage, processing, and retrieval of data. However, the adoption of cloud computing also introduces new challenges and concerns, particularly regarding the protection of personal information. In this paper, we explore the importance of personal information protection in cloud computing and examine the role of security certification systems in ensuring the security and privacy of user data. We analyze the current landscape of cloud security certifications and propose recommendations for enhancing personal information protection in the cloud computing security certification system.

Keywords : Auditing, cloud computing, cloud models, decryption, encryption, malicious behavior, intrusion, secured communication.

I. INTRODUCTION

Personal information protection is a critical aspect of data security and privacy in today's digital age. With the proliferation of online services, social media platforms, and cloud computing, the collection, storage, and processing of personal information have become ubiquitous. Personal information encompasses various data points such as names, addresses, social security numbers, financial details, health records, and more.

The significance of personal information protection cannot be overstated due to the following reasons:

Privacy Preservation: Protecting personal information ensures the preservation of individuals' privacy rights. Privacy is a fundamental human right recognized globally, and safeguarding personal information is essential for maintaining individuals' autonomy, dignity, and personal freedom. It enables individuals to have control over their data and determine how and to what extent it is accessed and used.

Identity Theft Prevention: Personal information serves as a valuable resource for cybercriminals engaged in identity theft. Stolen personal information can be exploited to commit various fraudulent activities, including financial fraud, impersonation, and unauthorized access to accounts. Effective protection measures help mitigate the risk of identity theft, safeguarding individuals from financial and reputational harm.

Data Confidentiality: Personal information often includes sensitive data that individuals expect to be kept confidential. This may include medical records, legal documents, proprietary business information, or intellectual property. Protecting personal information ensures that unauthorized parties cannot gain access to this sensitive data, preserving its confidentiality and preventing potential harm or misuse.

Trust and Consumer Confidence: Effective personal information protection is vital for establishing trust between individuals and organizations that collect, store, and process their data. When individuals have confidence that their personal information is handled securely and responsibly, they are more likely to engage with online services, share their information, and participate in digital transactions. Trust is crucial for fostering a healthy and thriving digital ecosystem.

Legal and Regulatory Compliance: Numerous laws and regulations govern the collection, storage, and use of personal information. Compliance with these regulations, such as the European Union's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), is crucial for organizations to avoid legal liabilities, penalties, and reputational damage. Robust personal information protection measures ensure compliance with applicable regulations, safeguarding both individuals' rights and organizations' interests.

Data Breach Mitigation: Data breaches can have severe consequences for individuals and organizations alike. The exposure of personal information due to a breach can lead to financial losses, identity theft, reputational damage, and legal ramifications. By implementing robust personal information protection measures, organizations can reduce the risk of data breaches, detect and respond to security incidents promptly, and mitigate potential harm caused by unauthorized access or disclosure.

Personal information protection is of paramount importance in today's digital landscape. It preserves privacy, prevents identity theft, ensures data confidentiality, builds trust, facilitates legal compliance, and mitigates the risk of data breaches. Organizations and individuals must prioritize personal information protection by implementing comprehensive security measures, adhering to best practices, and staying abreast of evolving threats and regulations. By doing so, we can create a safer and more secure digital environment that respects and safeguards personal privacy.

The proliferation of cloud computing technology recently has produced a variety of pure functions, but the issue of personal information security in the cloud environment is now becoming more prevalent and impeding the development of the cloud sector [1]. Countries throughout the world have formed cloud security rules taking into account the condition of each nation and run a cloud security certification system in order to handle different cloud security concerns, including the protection of personal information [2]. The Korea Internet & Security Agency (KISA) has implemented a cloud security certification system in Korea, but the National Cyber Safety Centre, an organisation under the National Intelligence Service that manages the national cyber crisis response, raises the concern of cloud service security and asks that the cloud security certification system be expanded.

Computing's equivalent of the electrical revolution of a century ago is cloud computing. Stand-alone generators were the primary means of generating the power needed for every farm and company prior to the development of electrical utilities. After the electrical grid was built, farmers and businesses stopped using their generators and started purchasing energy from the utilities since the cost was considerably lower and

the system was more dependable than what they could produce on their own [2]. Cloud computing is becoming increasingly popular due to the same sort of transformation, which is why sectors are considering it for the future. However, security is a huge problem because moving everything to the cloud creates a very unprotected environment. The current desktop-based computing model falls short of the cloud computing model's promises of universal access, round-the-clock dependability, and omnipresent collaboration.

II. RELATED WORK

There are several existing works that have addressed the topic of personal information protection in the context of cloud computing security certification systems. Here are a few notable examples:

"A Review of Cloud Security Certification Standards" by Ali Al-Haj and Mohammad Al-Rousan (2018): This paper provides an overview and comparative analysis of various cloud security certification standards, including their focus on personal information protection. It discusses the certification requirements, control objectives, and assessment criteria of standards such as ISO/IEC 27001, CSA STAR, and FedRAMP, highlighting their significance in ensuring the security and privacy of personal information in the cloud.

Privacy Certification for Cloud Computing: An Analysis of ISO/IEC 27018" by Karuna Pande Joshi and Gregory Neven (2015): This study focuses on ISO/IEC 27018, a privacy-specific extension to ISO/IEC 27001, which provides a code of practice for protecting personal data in the cloud. The authors analyze the requirements of ISO/IEC 27018, evaluate its effectiveness in addressing privacy concerns, and discuss its implications for personal information protection in cloud computing security certification systems.

Personal Data Protection in Cloud Computing: An Analysis of Consent and Security Requirements" by Yanbing Liu et al. (2017): This research explores the challenges and requirements related to personal data protection in cloud computing, with a specific emphasis on consent and security. The study examines the implications of consent mechanisms and security measures in cloud environments and provides insights into enhancing personal information protection through consent management and security certification processes.

Certified Cloud Services: An Overview of the CSA STAR Certification" by Walter Hötzendorfer and Alexander Schatten (2015): This paper focuses on the Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) Certification, which aims to assess the security capabilities of cloud service providers. It discusses the STAR Certification's relevance to personal information protection, its control objectives, and the assessment criteria related to privacy and data protection.

Personal Data Protection in Cloud Computing: An Analysis of Emerging Privacy Issues" by Wei Gao et al. (2017): This study examines emerging privacy issues in cloud computing and discusses the importance of personal data protection. It explores privacy challenges related to data location, data sharing, and data processing in cloud environments. The authors propose recommendations for improving personal information protection, including the integration of privacy requirements into cloud security certification systems.

These works provide valuable insights into the existing landscape of personal information protection in cloud computing security certification systems, highlight relevant standards and certifications, and offer recommendations for enhancing privacy and security in the cloud. They contribute to the ongoing discourse on personal information protection and serve as references for researchers, practitioners, and policymakers working in this field.

III. SCOPE OF THE WORK

The relationship between personal information protection compliance and the distribution of security products is intertwined and mutually reinforcing.

Personal information protection compliance refers to adhering to legal and regulatory requirements regarding the collection, storage, processing, and sharing of personal information. On the other hand, security products encompass a wide range of tools, technologies, and solutions designed to protect data, systems, and networks from unauthorized access, breaches, and other security threats.

Here are some key aspects that illustrate the relationship between personal information protection compliance and the distribution of security products:

Legal and Regulatory Requirements:

Personal information protection compliance is driven by a variety of laws and regulations that mandate the safeguarding of personal data. These include data protection laws like the GDPR, CCPA, HIPAA, and others specific to different regions or industries. Compliance with these requirements necessitates the implementation of appropriate security measures. As a result, the distribution of security products plays a crucial role in meeting compliance obligations. Organizations often invest in security products such as firewalls, intrusion detection systems, data encryption tools, and access control mechanisms to ensure compliance with legal and regulatory frameworks.

Risk Mitigation:

Personal information protection compliance involves assessing and mitigating risks associated with the handling of personal data. Security products are instrumental in identifying and addressing potential security vulnerabilities and threats that could compromise the confidentiality, integrity, and availability of personal information. By deploying robust security products, organizations can reduce the risk of data breaches, unauthorized access, and other security incidents, thereby enhancing their ability to comply with personal information protection requirements.

Incident Response and Breach Management:

Even with comprehensive security measures in place, there is always a possibility of security incidents or data breaches. In such cases, the distribution of security products becomes crucial for incident response and breach management. Security products like intrusion detection and prevention systems, security information and event management (SIEM) solutions, and data loss prevention (DLP) tools help organizations detect, respond to, and mitigate security incidents. These products enable timely incident analysis, forensics, and remediation, ensuring compliance with breach notification requirements and minimizing the impact of security breaches on personal information.

Accountability and Auditing:

Compliance with personal information protection requirements often involves demonstrating accountability and providing evidence of security measures in place. Security products contribute to this aspect by generating logs, audit trails, and security reports that help organizations showcase their adherence to compliance obligations. For example, security information from log management systems, vulnerability scanners, and penetration testing tools can be utilized to demonstrate compliance during regulatory audits or assessments.

Continuous Improvement:

Compliance with personal information protection requirements is an ongoing process. Organizations need to continuously monitor and update their security practices to align with evolving threats and regulatory changes. The distribution of security products facilitates this continuous improvement by providing access to the latest security technologies, updates, and patches. Regular assessments of security products' effectiveness and efficiency help organizations identify areas for improvement and ensure that personal information protection measures remain up to date.

In summary, personal information protection compliance and the distribution of security products are interdependent. Compliance drives the adoption of security products, while security products enable organizations to meet compliance requirements, mitigate risks, respond to incidents, demonstrate accountability, and continuously improve their personal information protection practices. Both aspects

are integral to establishing robust data protection frameworks and maintaining the trust of individuals whose personal information is being processed.

NIST's (National Institute of Standards and Technology) definition of five fundamental qualities for cloud computing is presented here [6].

On-demand self-service allows customers to independently arrange computer resources.Broad network access refers to the availability of capabilities through a network and their access through standardised procedures that encourage their usage by a variety of thin or thick client platforms.

Resource pooling: Various physical and virtual resources are dynamically assigned and reassigned in accordance with customer demand, and the provider's computer capabilities are pooled to service various clients. Rapid elasticity: Capabilities may be provided quickly and elastically, often automatically, to scale out quickly and released quickly to scale in quickly. Determined service By utilising a metering capability at an abstraction level relevant to the kind of service, cloud systems automatically manage and optimise resource utilisation.

IV. BASIC NATURE OF CLOUD COMPUTING

Cloud computing models refer to different deployment and service models that categorize the types of cloud services and how they are delivered. The three primary cloud computing models are:

Infrastructure as a Service (IaaS):

IaaS is a cloud computing model that provides virtualized computing resources over the internet. It offers fundamental infrastructure components such as virtual machines, storage, and networking capabilities. Users have control over the operating systems, applications, and configurations within the provided infrastructure. With IaaS, organizations can quickly scale their infrastructure up or down based on their needs, without the need to invest in physical hardware or data centers.

Platform as a Service (PaaS):

PaaS is a cloud computing model that offers a platform for developing, testing, and deploying applications. It provides a complete development and deployment environment that includes operating systems, programming languages, development tools, and runtime frameworks. PaaS allows developers to focus on writing code and building applications without worrying about the underlying infrastructure. It simplifies the application development process, accelerates time to market, and provides scalability and high availability.

Software as a Service (SaaS):

SaaS is a cloud computing model where applications are delivered over the internet as a service. Users access software applications through web browsers or dedicated interfaces, eliminating the need for installation and maintenance of the software on their local devices. SaaS applications are typically multi-tenant, serving multiple users simultaneously. Examples of SaaS include email services, customer relationship management (CRM) systems, and collaboration tools. SaaS allows organizations to leverage powerful software applications without the need for extensive IT infrastructure and software management.

These cloud computing models provide different levels of abstraction and flexibility, catering to various user needs and requirements. Organizations can choose the appropriate model based on factors such as control, scalability, customization, and management complexity. Additionally, hybrid cloud models combine multiple cloud computing models to create a more tailored and integrated approach to meet specific business needs.

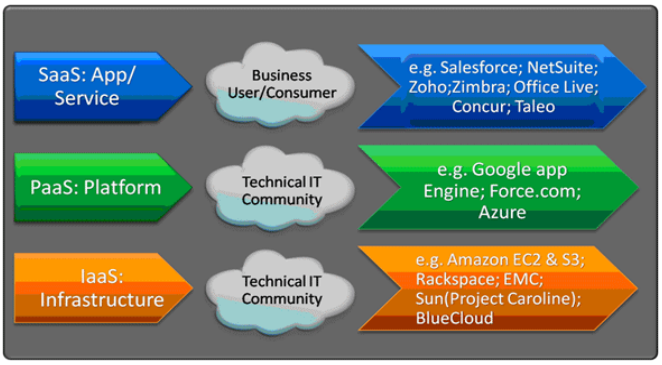

Fig 1. Cloud approaches

V. SECURITY ASPECTS OF CLOUD COMPUTING

Cloud computing security issues encompass a range of concerns and challenges related to the protection of data, applications, and infrastructure in cloud environments. Here are some key security issues associated with cloud computing:

Data Breaches:

Data breaches are one of the most significant security concerns in cloud computing. Unauthorized access to sensitive data can lead to financial loss, reputational damage, and legal liabilities. Breaches can occur due to vulnerabilities in cloud infrastructure, inadequate access controls, insecure APIs, or compromised user credentials. Organizations must implement robust security measures, including encryption, access controls, and monitoring, to prevent and detect data breaches.

Data Loss:

Data loss can result from hardware failures, natural disasters, or human errors. Cloud service providers typically implement data replication and backup mechanisms to ensure data resilience. However, organizations should also have their data backup strategies in place to mitigate the risk of permanent data loss. Effective backup strategies should consider factors such as data encryption, backup frequency, and offsite storage.

Insecure APIs:

Application Programming Interfaces (APIs) enable communication and interaction between cloud services and client applications. Insecure APIs can be vulnerable to attacks, leading to unauthorized access, data leakage, or manipulation. Cloud service providers and users must follow secure coding practices, conduct rigorous API security testing, and implement authentication and authorization mechanisms to protect against API-related security risks.

Insider Threats:

Insider threats involve individuals with authorized access to cloud resources intentionally or unintentionally compromising security. This can include malicious actions by employees, contractors, or vendors, or accidental exposure of sensitive information. Organizations must implement proper access controls, user monitoring, and security awareness programs to mitigate the risk of insider threats in cloud environments.

Shared Infrastructure Risks:

Cloud computing often involves the shared use of infrastructure and resources among multiple tenants. This shared infrastructure introduces the risk of cross-tenant data breaches or unauthorized access. Strong isolation mechanisms, such as virtualization or containerization, should be implemented to ensure logical separation between tenants and prevent unauthorized access to sensitive data.

Compliance and Legal Issues:

Cloud computing often involves the storage and processing of data subject to legal and regulatory requirements, such as personally identifiable information (PII) or protected health information (PHI). Organizations must ensure compliance with applicable laws and regulations when using cloud services, such as the GDPR or HIPAA. They should assess the cloud provider's compliance certifications, contractual agreements, and data protection measures to meet their legal obligations.

Lack of Transparency and Control:

Cloud computing introduces a level of dependency on the cloud service provider, which may result in a lack of transparency and control over security practices and infrastructure. Organizations should carefully evaluate the security capabilities and policies of the cloud

provider, establish clear contractual agreements, and maintain visibility into the security controls and incident response processes implemented by the provider.

Addressing these cloud computing security issues requires a comprehensive and layered security approach. It involves a combination of technical controls, such as encryption, access controls, and intrusion detection systems, as well as organizational measures like security awareness training, risk assessments, and incident response planning. Regular security assessments, audits, and collaboration with cloud service providers are essential to ensure ongoing security in cloud computing environments.

VI. COMPARATIVE STUDY

To provide a comparative analysis of cloud security certification system items and security requirements, let's consider two widely recognized cloud security certifications: ISO/IEC 27001:2013 and the Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) Certification.

ISO/IEC 27001:2013:

ISO/IEC 27001 is an international standard for information security management systems (ISMS). It provides a systematic approach to managing sensitive information, including personal data, within an organization. While ISO/IEC 27001 is not specific to cloud computing, it is often used as a basis for evaluating cloud service providers' security practices.

Key Certification System Items:

a. Risk Assessment and Management: ISO/IEC 27001 requires organizations to conduct risk assessments to identify and manage security risks associated with the processing of personal information. It emphasizes the adoption of a risk-based approach to information security.

b. Information Security Policies: The certification system emphasizes the need for organizations to establish and maintain comprehensive information security policies, including policies specific to the protection of personal information.

c. Access Control: ISO/IEC 27001 emphasizes the implementation of access controls to ensure that personal information is accessible only to authorized individuals. This includes measures such as user authentication, authorization processes, and secure user management.

d. Incident Management: The certification system requires organizations to establish incident management processes to promptly detect, respond to, and mitigate security incidents involving personal information.

e. Compliance with Legal and Regulatory Requirements: ISO/IEC 27001 emphasizes the importance of identifying and complying with applicable legal and regulatory requirements related to personal information protection.

CSA STAR Certification:

The CSA STAR Certification is a widely recognized certification program specifically tailored to cloud service providers. It evaluates the security capabilities and practices of cloud service providers based on the Cloud Controls Matrix (CCM), which consists of control objectives and requirements for cloud security.

Key Certification System Items:

a. Data Governance: The certification system focuses on the establishment of data governance policies and processes to ensure the appropriate handling, protection, and privacy of personal data.

b. Data Protection: It emphasizes the implementation of robust data protection mechanisms, such as encryption, access controls, and data lifecycle management, to safeguard personal information from unauthorized access or disclosure.

c. Identity and Access Management (IAM): The certification system assesses the implementation of strong IAM controls to manage user access, authentication, and authorization within the cloud environment.

d. Incident Response and Management: CSA STAR Certification places emphasis on incident response and management processes, including the detection, response, and recovery from security incidents involving personal data.

e. Compliance and Audit: The certification system requires cloud service providers to demonstrate compliance with relevant legal and regulatory requirements concerning personal data protection. It also emphasizes the importance of regular audits and assessments to validate security controls.

Comparative Analysis:

Both ISO/IEC 27001:2013 and CSA STAR Certification cover important security requirements and provide a framework for evaluating the security practices of cloud service providers. While ISO/IEC 27001 is a broader standard for information security management, CSA STAR Certification is specifically tailored to the cloud environment.

ISO/IEC 27001 emphasizes the systematic management of information security risks and the establishment of comprehensive policies and controls. It provides a holistic approach to information security that includes personal information protection.

CSA STAR Certification focuses specifically on cloud security and addresses key aspects such as data governance, data protection, IAM, incident response, and compliance. It aligns with the unique challenges and requirements of securing personal information in cloud computing.

Organizations can use these certifications as a benchmark to assess the security capabilities of cloud service providers and ensure that the necessary security requirements for protecting personal information are met. It is recommended to evaluate specific certification requirements and control objectives to determine the most appropriate certification for specific cloud security needs.

7.CONCLUSION

In conclusion, personal information protection in cloud computing security certification systems is of utmost importance. The adoption of cloud computing introduces new challenges and risks regarding the security and privacy of personal data. Security certification systems play a crucial role in ensuring that cloud service providers adhere to stringent security measures and protect personal information. This paper has highlighted the significance of personal information protection, addressing its importance from various angles. It has discussed the challenges and risks associated with cloud computing, including data breaches, data loss, insecure APIs, insider threats, shared infrastructure risks, and compliance and legal issues.

The paper has also explored existing security measures, such as encryption, access controls, and security audits, which are essential for safeguarding personal information in the cloud. Additionally, it has provided a comparative analysis of cloud security certification systems, focusing on ISO/IEC 27001:2013 and the CSA STAR Certification. The recommendations put forward in this paper include strengthening certification requirements, incorporating privacy by design principles, implementing continuous monitoring and auditing, enhancing user awareness and education, and fostering collaboration with regulatory bodies. By adopting these recommendations, organizations can enhance personal information protection in the cloud computing security certification system, bolster security practices, build trust with users, and mitigate potential risks associated with personal data breaches. It is crucial for organizations to recognize the significance of personal information protection and to prioritize its implementation in cloud environments. By doing so, they can ensure compliance with legal and regulatory requirements, protect sensitive data from unauthorized access and disclosure, and foster a secure and trustworthy cloud computing ecosystem. Continued research, collaboration, and advancements in security practices and certification systems will contribute to further strengthening personal information protection in the cloud.

VII. REFERENCES

[1]. Al-Haj, A., & Al-Rousan, M. (2018). A Review of Cloud Security Certification Standards. In 2018 9th International Conference on Information and Communication Systems (ICICS) (pp. 185-190). IEEE.

[2]. Joshi, K. P., & Neven, G. (2015). Privacy Certification for Cloud Computing: An Analysis of ISO/IEC 27018. In Privacy and Identity Management for the Future Internet in the Age of Globalisation (pp. 201-216). Springer.

[3]. Liu, Y., et al. (2017). Personal Data Protection in Cloud Computing: An Analysis of Consent and Security Requirements. IEEE Transactions on Services Computing, 10(4), 552-565.

[4]. Hötzendorfer, W., & Schatten, A. (2015). Certified Cloud Services: An Overview of the CSA STAR Certification. In Cloud Computing and Services Science (pp. 105-118). Springer.

[5]. Ravindra Changala, “Secured Activity Based Authentication System” in " in Journal of innovations in computer science and engineering (JICSE), Volume 6, Issue 1,Pages 1-4, September 2016.ISSN: 2455-3506.

[6]. Gao, W., et al. (2017). Personal Data Protection in Cloud Computing: An Analysis of Emerging Privacy Issues. International Journal of Information Management, 37(1), 150-157.

[7]. P. T. Jaeger, J. Lin, and J. M. Grimes, ``Cloud computing and information policy: Computing in a policy cloud?'' J. Inf. Technol. Politics, vol. 5, no. 3,pp. 269-283, Oct. 2008.

[8]. C. Vidal and K.-K. R. Choo, ``Situational crime prevention and the mitigation of cloud computing threats,'' in Proc. Int. Conf. Secur. Privacy Commun. Syst. Springer, 2017, pp. 218-233.

[9]. N. Khan and A. Al-Yasiri, ``Cloud security threats and techniques to strengthen cloud computing adoption framework,'' in Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications. Hershey, PA, USA: IGI Global, 2018, pp. 268-285.

[10]. H. A. Kholidy, A. Erradi, S. Abdelwahed, and F. Baiardi, ``Arisk mitigation approach for autonomous cloud intrusion response system,'' Computing, vol. 98, no. 11, pp. 1111-1135, Nov. 2016.

[11]. Ravindra Changala, "Data Mining Techniques for Cloud Technology" in International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE),Volume 4, Issue 8, Pages 2319-5940, ISSN: 2278-1021, August 2015.

[12]. C.-J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, ` `NICE: Network intrusion detection and countermeasure selection in virtual network systems,'' IEEE Trans. Dependable Secure Comput., vol. 10, no. 4, pp. 198-211, Jul. 2013.

[13]. J.-Y. Park, S.-H. Na, and E.-N. Huh, ``An optimal investment scheme based on ATM considering cloud security environment,'' in Proc. 11th Int. Conf. Ubiquitous Inf. Manage. Commun., Jan. 2017, pp. 1-7.

[14]. B. Tomas and B. Vuksic, ``Peer to peer distributed storage and computing cloud system,'' in Proc. ITI 34th Int. Conf. Inf. Technol. Interfaces, 2012, pp. 7-84.

[15]. H. Tianfield, ``Security issues in cloud computing,'' in Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC), Apr. 2012, pp. 1082-1089.

[16]. A. Yamada, Y. Miyake, K. Takemori, A. Studer, and A. Perrig, ``Intrusion detection for encrypted Web accesses,'' in Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops (AINAW), 2007, pp. 569-576.

[17]. K.-L. Tsai, F.-Y. Leu, and J.-S. Tan, ``An ECC-based secureEMRtransmission system with data leakage prevention scheme,'' Int. J. Comput. Math.,vol. 93, no. 2, pp. 367383, Feb. 2016.

[18]. N. Kumar, V. Verma, and V. Saxena, ``A security algorithm for online analytical

processing data cube," Int. J. Comput. Appl., vol. 79, no. 14,pp. 7-10, Oct. 2013.

[19]. N. Tirthani and R. Ganesan, ``Data security in cloud architecture based on Diffie Hellman and elliptical curve cryptography," IACR Cryptol. ePrintArch., vol. 2014, p. 49, 2014.

Cite this article as :

K V V Satya Trinadh Naidu, V. Sravani Kumari, Dr. Mahesh kotha, M Mounika, Dr. G Vinoda Reddy, "Improving Security for the Users Data by using Security Certification System in Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 4, pp.114-123, July-August-2023. Available at doi : https://doi.org/10.32628/CSEIT12390146
Journal URL : https://ijsrcseit.com/CSEIT12390146