International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I3P206

Volume 69 Issue 3, 29-33, March 2021
© 2021 Seventh Sense Research Group®

A Structured Protective Cohesive Health Care Information System Using Security And Storage Mechanism In Cloud

Srinivasan S[1], Sanjeev Kumar Mandal[2] , Lalit Kumar[3] , Menaka C[4] , Akhil Arun Menon[5]

[1,4] *Associate Professor, Dept of BCA, School of Computer Science & IT, Jain Deemed to be University, Bengaluru, India*
[2,3,5] *Assistant Professor, Dept of BCA, School of Computer Science & IT, Jain Deemed to be University, Bengaluru, India*

s.srinivasan@jainuniversity.ac.in, km.sanjeev@jainuniversity.ac.in, k.lalit@jainuniversity.ac.in

Abstract *- Nowadays, information technologies focusing on the user and data security along with perfect data storages are the key factor in emerging cloud-based computer technology. The present methods manage the privacy and protection concern includes user and data authentication with multiple cloud-based online-storages. This paper focusing the information technology-based safety concern comprises loss of secret information, data integrity, confidentiality, data availability while the distribution of user's secret data in a cloud-based protective environment. Allocation of resources and storing of secret data are highly vulnerable to various cyber-based attacks, which bring permanent heavy data and loss of confidential information in the health care system. In order to overwhelm the above things, nowadays, the cloud providers and consumers required high performance, protective cohesive health care management information system which conveys reliable online as well as an offline backup like the redundant array of independent disk storage with user and data authentication mechanism in internet-based cloud computing. This paper also deals with the perfect tunnel-based data movement control by advanced improved rule-based methods along with storing confidential health care information in distinguished storage through a cryptographic mechanism insecure manner. This paper also deals with the prevention techniques of cross-site scripting attacks, which able to prevent information and afford security against internet-based web-based attacks. This protected cohesive health care information confirms the data integrity, security, data availability and also firmly insists on the multi-tier cloud-based architecture. This method raises various users' spirits and morals from clerical to executive members that meet their needs and recognize the defendable development of internet-based health care management information system. This capable secured health care system maintains enhanced performance evaluation in terms of the reduced huge number of attacks and comparison of uploading time in cloud storages, consumer queried rate, bandwidth consumption with different approaches. This method assures better availability of data, privacy, and security on internet-based protective health-care management information systems.*

Keywords: *Authentication, Attacks, Confidentiality, Cohesive, Health-care, Integrity;*

I. INTRODUCTION

Cloud is a familiar worldwide topic in internet-based computing technologies. It enables well-controlled online-services, sharing of user demand resources, customized oriented business, and management-based applications [1]. The health care management information system is a web-oriented application wished-for each tailor-made consumer to store and share confidential information remotely. The internet-based health-care system achieves goals efficiently and emphasizes sharing of interactive original information ideas in integrated knowledge-based computing technologies [2].

Cloud provides glorious online-storages for many internet-based insurances as well as hospital-oriented application systems. It permits well-organized distributed computing facilities by centralizing storage capabilities with a high-speed processing information system [3]. Cloud security insists on standards, methods, and well-equipped technologies that protected secret health care diagnosis and its related insurance information with the accompanying arrangement services and infrastructure along with privacy procedures and data storage centers [4]. Currently, several discrete techniques are available for the consistent medicinal-based application that need perfect authentication, efficient online as well as offline storage for enhancing client's interoperability among health care information services.

The key objective is to create perfect innovative a secure, cohesive internet-based health-care management information that provides the combination of customized clients authentication security method, multi-variant distinguished data storages with secured tunnel-based data flow information control passing method that guarantee confidentially, data leakage, user verification, and validation with data integrity.

II. LITERATURE SURVEY

The most probable challenges of the cloud are data escape, threats, attacks, flaws, user authentication, data intrusion, confidentiality, data availability, data integrity, and many more unknown issues that have appeared while consumers sharing their identical information such as credit card confidential details, health insurance details are stored in distributed identical locations [5].

Presently hospital-based patient health care and insurance-based information server giving perfect customized user demand fit-made services through cloud-based applications from different cloud-based online storages with back-up capacity as well as cloud experts service providers concerning types of types [6, 7].

The cryptographic mechanism applied in transport layer security and secure socket layer, which give data security between peer-to-peer points in the cloud that inform generous control overhead due to computer processing time [8].

Presently the huge and vast growth of information technology concerning increasing in cost computation, data storage, and establishment of a connection between cloud providers and consumers, so the fast growth of computer-based information technology is directly proportional to the threats, flaws, and attacks [9]. Therefore, user's security, confidentiality, and privacy are major key concerns of health-care internet-based computing technology [10]. Web-based threats and attacks and injection vulnerabilities such as cross-site scripting are the present issues cloud.

Zeller et al. [11] represent cross-site scripting (CSS) and cross-site request forgery (CSRF) web-based attacks and their preventive actions and recommend internet-based web server information changes that enable to check and prevent the web domain from web-based attacks. Cachin et al. [12] show the different types of various risks, threats from different areas. The cloud security challenges and issues are shown in Figure 1.1.

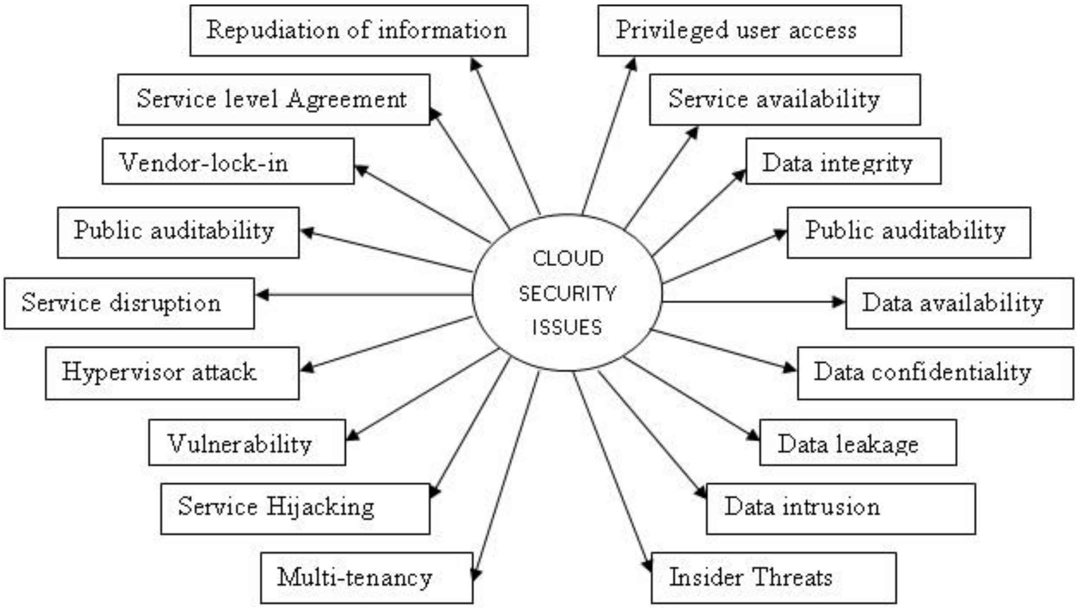

Figure 1.1 Cloud security challenges and issues

Farhan Bashir Shaikh et al. [13] suggested various methods which focused on issues of privacy, confidentiality, and security in the cloud.

III. PROTECTIVE COHESIVE HEALTH CARE INFORMATION SYSTEM IN THE CLOUD

The protective cohesive information system implements multifaceted structural architecture as user interface, business transaction, and information storage layers. The predominant researchers proposed extra-ordinary security with high-performance computing standards and models even though some levels of security features and user privacy issues are still available. The protective cohesive health care information system in cloud computing architecture is shown in Figure 1.2.

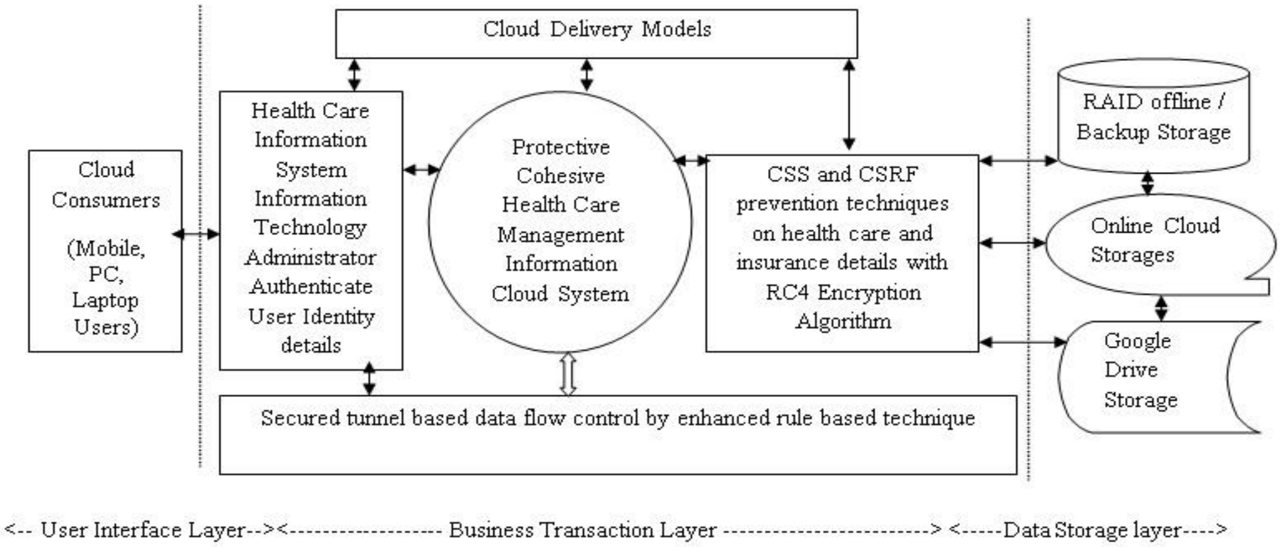
Cloud Delivery Models
Cloud Consumers (Mobile, PC, Laptop Users)
Health Care Information System Information Technology Administrator Authenticate User Identity details
Protective Cohesive Health Care Management Information Cloud System
CSS and CSRF prevention techniques on health care and insurance details with RC4 Encryption Algorithm
RAID offline / Backup Storage
Online Cloud Storages
Google Drive Storage
Secured tunnel based data flow control by enhanced rule based technique
<-- User Interface Layer--><------------------ Business Transaction Layer ------------------------> <-----Data Storage layer---->

Figure 1.2 Structure of Protective Cohesive Health Care Information System in Cloud

The cloud consumer may use their mobile phones or desktop computer or laptop or tablet to access the secure, interconnected health care management information internet-based cloud computing. The user interface layer occupied the identity details of cloud clients. Any two identity details like one-time passcode or quick response passcode or mobile passcode or user email-id secret code must be verified and validated for accessing and storing the confidential health care or insurance details of medical treatment-claim details of cloud-based secure health-care information system. The public cloud can be used by all users.

To make sure of secured data flow control through an enriched rule-based technique which maintains user privacy and give more access permission with Priority-based security constraints to the various user's transmission of secret information among users and third-party service providers. This modernized, enhanced rule technique deploys a customized group of procedures or rules which monitor and control user activities and also prevent the system from malicious users' actions [14].

The cloud consumer's health care or insurance details are stored in online cloud storage like CloudMe or AWS S3 storage or Google-drive and offline backup storage in the form of RC4 cryptographic based algorithm with the assistance of public and private cloud service providers like Amazon cloud storage services. This RC4 performs two phases as initialization and operation which

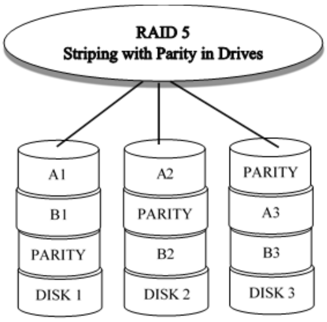

Figure 1.3 RAID Interleaved Stripping with Parity across Drive in Disk

Encrypting the health care details and also decrypt it in storages like online/offline and Google drive division that utilizing interleaved striping of dispersed equal parts of the drive with parity enclosing information and achieved high level of redundancy because of division striping and dispersed parity mechanism as shown in Figure 1.3.

The http-request and top-secret cookie preference diminish input techniques are the standard cross-site scripting preventive scheme which able to prohibits web-application oriented attacks and also to prevent vulnerable tags, web-based attacks, threats, and harmful, malicious codes generated by hackers and storing truthful and validated confidential health-care information in distinct data storages [16,17].

IV. RESULTS AND DISCUSSION

The most important objective of Structured Cohesive Health-care management Information System (CHIS) is to establish prospered trust-based protective security and storage methods that conserve safeguard well-equipped enhanced rule-based functionalities with the cryptographic mechanism in a cloud environment. This secure system develops the extraordinary computing performance and evaluation of health-care information. These CHIS apply the preventive mechanism of internet-based attacks and protect health-care insurance claim confidential details from malicious user's web-based attacks and also resolved the challenges of the cloud such as data leakage, privacy, user authentication, and security in a cloud environment.
This CHIS cloud-based system attained better (maximum of 62%) bandwidth consumption, comparison of uploading time of files in online and offline backup data storages, comparison of consumer user queried rate (attained highest of 55%) with several methods like PPV, HASSM, and reduced more than 85% enormous quantity of internet-based attacks in this cloud environment.

The bandwidth consumption is well-defined as the bit frequency consumed to pass the information cloud. The bandwidth usage of the proposed CHIS is compared with other approaches like Probabilistic query and Periodic Verification method (PPV) and Homomorphism Authenticators using Sphere Shaped Marker (HASSM), and the standard value shows that improved bandwidth usage is gained for the CHIS EMHT method as depicted in Figure 1.4.

storages [15].
The consumers also store their secret details in a redundant array of independent disks storage is an extraordinary offline back storage which combined joins a few circles smashes into a consistent

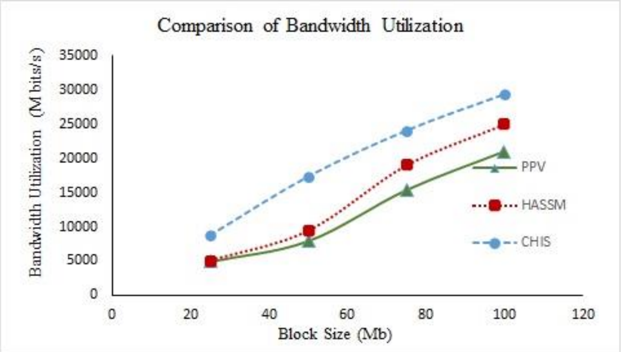

Figure 1.4 Comparison of bandwidth usage with PPV and HASSM approaches

Figure 1.4 represents the values of bandwidth usage (M bits/sec) for the respective size of the file in a megabyte. The employment of bandwidth rate of CHIS is enlarged by least of 24%, and extreme of 49% is compared with HASSM, which is also likewise 42% - 61% with PPV. The disparate size of files can be uploaded in different online and offline cloud storages through the internet, with the respective uploading time is represented in Figure 1.5

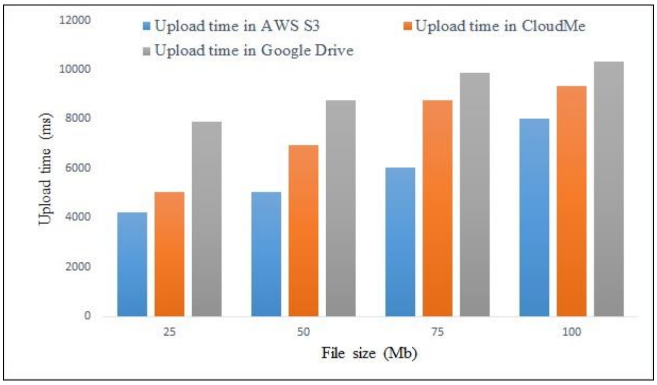

Figure 1.5 Comparison of Uploading time in Online Cloud Storages

The uploading time of files was less in AWS S3 cloud storage compared to CloudMe and Google drive. The AWS S3 cloud storage takes the lowest of 30% - an extreme 50% less of uploading time compared with Google drive and similarly minimum of 20% to a maximum of 30% less uploading time compared with CloudMe.

The consumer queried rate of CHIS is compared with PPV, and HASSM approaches are portrayed in Figure 1.6

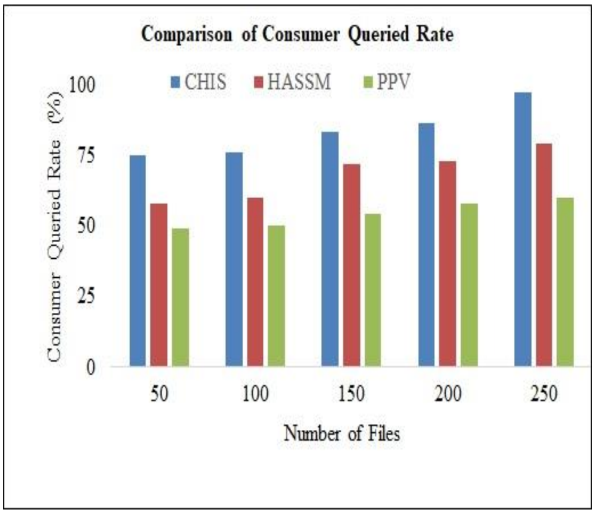

Figure 1.6 Comparison of Consumer Queried Rate with PPV and HASSM

The consumer queried rate shows a quantity of positive, successful value in making exact perfect results to users. The users' files can be verified by CHIS method and enlarged the progress of queried rate by 35% - 55% when associated with PPV method and similarly compared lowest of 10% and highest of 31% is enlarged of consumer queried rate with HASSM.

V. CONCLUSION AND FUTURE ENHANCEMENT

To safeguard the confidential cloud-based digital data, secret pieces of information, and sharing of resources and services in digital library systems against vulnerability and flaws. Therefore, proposed innovative and interoperable cloud-based integrated digital library secure methods which make information are more secured by authenticating the various users and auditing the digital resources are essential for reducing attacks and unauthorized user's access. This paper confirmed the integrated digital library secured authentication methods like a one-time password or email-id and quick response code, which scrutinized cloud user's verification and validation.

This method proposed an audit method that enforces verifying and auditing the digital library resources through the *k*-means cluster technique. The adaptive integrated digital library methods were storing secret data and other cloud resources on different cloud storages and back up storages through RC4 and another encryption method. This method was monitoring the user's confidential, secret data and controlling the flow of information through the enriched rule-based method in the cloud. It also implements Netdata and Cloudify, which monitoring and managing the activities and events of the cloud in public/private digital libraries. This paper reduces an enormous number of threats, vulnerabilities, and flaws, comparison of CHIS method with other approaches like PPV and HASSM with respect to client queried rate, bandwidth utilization, and storing of user's resources in cloud storages. It achieved better user verification and also solved the issues of data loss, availability of data, user privacy, and data integrity in a structured protective cohesive health care cloud environment. In the future, the standard hardware interfaces and wireless-based devices will be incorporated in this cloud-based health-care infrastructure information system.

VI. REFERENCES

[1] Guoman Lin, Research on Electronic Data Security Strategy Based on Cloud Computing, 2012 IEEE second International conference on Consumer Electronics, ISBN: 978-1-4577-1415-3, 1228-1231 (2012).

[2] Kannan. K, Raja. K, Secure Decision-Making Approach to Improve Knowledge Management Based on Online Samples", International Journal of Intelligent Engineering and Systems, 11(1)(2018) 50-61, DOI: 10.22266/ijies2018.0228.06.

[3] Akhil Behl, Kanika Behl, An Analysis of Cloud Computing Security Issues, 2012 IEEE proceedings World Congress on Information and Communication Technologies, (2012) ISBN: 978-1-4673-4805-8,109-114.

[4] Deyan Chen, Hong Zhao, Data Security and Privacy Protection Issues in Cloud Computing,2012 IEEE proceedings of International Conference on Computer Science and Electronics Engineering, ISBN: 978-0-7695-4647-6,(2012) 647-651.

[5] Rajkumar Sharma et al., An Intelligent Cloud Computing Architecture Supporting e-Governance, proceedings of the 17th International Conference on Automation & Computing, University of Huddersfield, (2011) 1-5,10th.

[6] Srinivasan. S, K.Raja, An Advanced Dynamic Authentic Security Method for Cloud Computing, In Bokhari M., Agrawal N., Saini D. (Eds), Cyber Security - Advances in Intelligent Systems and Computing (AISC) Book Series,729(2018) 143-152, Springer, Singapore.

[7] M. Auxilia, K. Raja, K. Kannan, Cloud-Based Access Control Framework for Effective Role Provisioning in Business Application" International Journal of System Dynamics Applications, IGI-Global USA, 9(1)(2020) 63-80.

[8] Y. Zhong et al., A Self-Adaptive Encryption and Decryption Architecture, IEEE International Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), Xiamen, China, (2019) 388-397.

[9] Arul Rajakumar, Rajalakshmi Shenbaga Moorthy, and Ali Kashif Bashir, "Ensemble Learning Mechanisms for Threat Detection: A Survey, Machine Learning, and Cognitive Science Applications in Cyber Security, USA, (2019) 240-281.

[10] Swathy R, Vinayagasundaram B, Rajesh G, Nayyar A, Abouhawwash M, Abu Elsoud M, Game theoretical approach for load balancing using SGMLB model in cloud environment" PLoS One 15(4)(2020).

[11] Zeller W, Felten EW. Cross-Site Request Forgeries: Exploitation and Prevention, (2008) 1-13 http://citp.princeton.edu/csrf.

[12] C.Cachin, I. Keidar, and A. Shraer Trusting the cloud, ACM SIGACT News,40(2009) 81-86.

[13] Farhan Bashir Shaikh, Sajjad Haider, Security Threats in Cloud Computing, Proceedings of the 6th International Conference on Internet Technology and Secured Transactions, IEEE, (2011).

[14] Srinivasan.S, K.Raja, Trusted Integrated Security Mechanism for Reducing Vulnerability using Authentic and Auditing Methods in Cloud Computing, International Journal of Pure and Applied Mathematics, 119(12)(2018).

[15] Jian Xie, Xiaozhong Pan, An improved RC4 stream cipher, Proceedings of the International Conference on Computer Application and System Modelling IEEE, (2010) 156-159.

[16] S.Srinivasan, K.Raja, Preventing Cloud Attacks using Bio-Metric Authentication in Cloud Computing, Indian Journal of Science and Technology, 9(23)(2016) DOI:10.17485/ijst/2016/v9i23/88322.

[17] Srinivasan. S, K.Raja, An Advanced Dynamic Authentic Security Method for Cloud Computing", In Bokhari M., Agrawal N., Saini D. (eds) Cyber Security - Advances in Intelligent Systems and Computing(AISC) Book Series, 729(2018) 143-152, Springer, Singapore.