An Advanced Dynamic Authentic Security Method for Cloud Computing

S. Srinivasan and K. Raja

Abstract Cloud computing delivers a broad range of services and resources like computational power, storage, computational platforms, and applications to cloud consumers through the Internet by on demand, pay-per-usage basics. With a growing number of cloud service providers resorting to using and sharing resources in the cloud environment, there is a necessity for protecting the data of various users from unauthorized access of information between network and cloud. However, the security and privacy of an open-ended, reasonably sharing of accessible resources is still uncertainty and present a major complication for cloud consumers to acclimatize interested in cloud environment. This manuscript initiates and deeply examines the cloud security problem. This paper deals with the protection concern that includes many of the cloud attacks, data integrity, data leakage, privacy, confidentiality, vulnerabilities during sharing of resources, services, and information. This method deals with securing the cloud information without data loss from malicious users, hackers, and attackers of a real-time environment. This method verifies user authentication and authorization management. It assures security on the transmission of data, quality of service, and prevents vital information from various active and passive attacks. This proficient method preserves the cloud environment with better performance evaluation. Furthermore, security and privacy analysis know the ability of the proposed method for cloud computing and extend productive efficiency with safe cloud computing environments.

Keywords Cloud security · Data integrity · Authentication · Vulnerabilities Attacks

S. Srinivasan (✉)
Research Development Center, Bharathiar University, Coimbatore, Tamilnadu, India
e-mail: effectivemail@yahoo.com

S. Srinivasan
Department of M.C.A, K.C.G College of Technology, Chennai, Tamilnadu, India

K. Raja
Alpha College of Engineering, Chennai, Tamilnadu, India
e-mail: raja_koth@yahoo.co.in

M. U. Bokhari et al. (eds.), *Cyber Security*, Advances in Intelligent Systems and Computing 729, https://doi.org/10.1007/978-981-10-8536-9_15

1 Introduction to Cloud Environment

Presently, cloud environment is a rapidly increasing novel information technology of computer industry, which has produced the concern of the entire world. It is the derivative of a large-scale distributed computing with Internet-based technology [1]. Cloud computing environment is also a novel approach to computational business computing, in which software, hardware, services, other resources are shared and provided to computers by a pay-per-usage computed service through the internetwork. It facilitates users to access storage, information, and resources online via Internet [2]. Moreover, cloud computing offering fault-tolerant services with improved better performance and provides an identity management mechanism for millions of users simultaneously [3].

The cloud service providers have Infrastructure as a Service, Platform as a Service, Software as Service, and several services to present. A cloud environment has several characteristics such as on-required service, resource collections, elasticity, and calculated measured service. The significant features of cloud environment are elasticity, scalability, multi-tenancy, self-provisioning of resources, and on-demand self-service [4].

A cloud can be public, private, community, and hybrid cloud. According to new information technologies (IT) and business models, the cloud computing infrastructures and applications have been developed rapidly and the security is the major consideration for the customer to adopt cloud computing. Cloud environment focuses on sharing consumers data, information, and calculations over the Internet computing clients such as computers, data storage centers, and cloud computing services. It allows efficient computing capabilities by centralizing global storage,

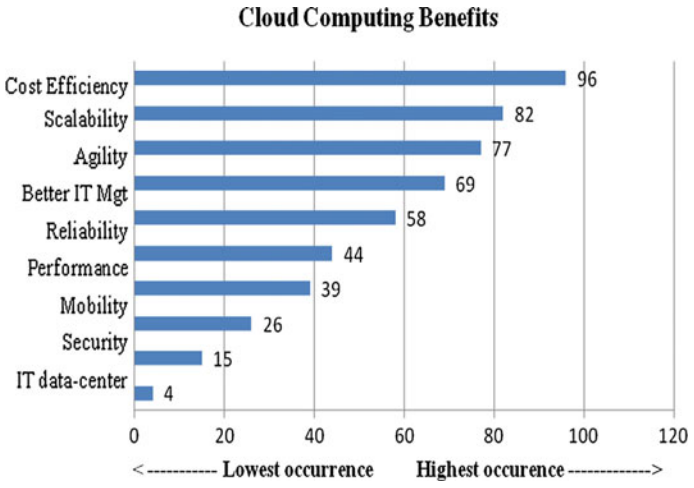

Fig. 1 Benefits of cloud computing

processing, and bandwidth. The benefits [4, 5] of cloud environment are shown in Fig. 1.

In a cloud environment, security and privacy are shared between the cloud service providers and consumers. The main problem of the cloud environment is a large number of security threats, cloud attacks, hijacking of network information on outsourcing of resources as well as business-critical process and data. Some security issues in the cloud are data integrity, information confidentiality, data leakage, vulnerability, and data intrusion. To ensure facts' confidentially, information integrity and availability, the cloud provider provides that at a minimum, include the following:

- Cryptographic method to guarantee that the shared and global data centers secured all information.
- Strong user access technique and user authentication methods to protect against illegal contact to the data.

Cloud computing security [5] is a large set of security controls, strong policies, recent technologies, and methods set to safeguard the data and applications of the cloud environment. The rest of this chapter is ordered as follows: Sect. 2 discusses cloud security risks and issues. Section 3 gives a detailed description of the proposed exciting advanced dynamic authentic security method for cloud computing. Section 4 shows the performance of experimental and their interpretation outcome. Finally, Sect. 5 concludes the paper and further improvements.

2 Security Risks and Challenges in Cloud

Security and privacy concerns indicate in the implementation of cloud computing technologies for sharing of information, resources, services, and data storage. Protecting the cloud data such as sharing of resources, user identification like credit and debit card details from the malicious insider is a foremost impact in cloud. Garfinkel [6] identified data intrusion may happen with the cloud service providers, like Amazon service, is data intrusion. A cloud security [7] is the most responding in the percentage of the challenge of nine issues recognized to cloud environment as shown in Fig. 2.

In cloud, security and privacy events are observed and mentioned below [7]:

- A salesforce.com employee fell prey to a phishing attack, which leads to loss of data that produced further during the year 2007.

According to Akhil Behl [4], Data loss is major security challenges raised by the users. When the IT companies or organizations transfer their confidential information to cloud, the cloud service provider is not able to undertake the security and data integrity as they would in their location, that cause data leakage and loss of control due to multi-tenant strategy maintained in cloud computing.

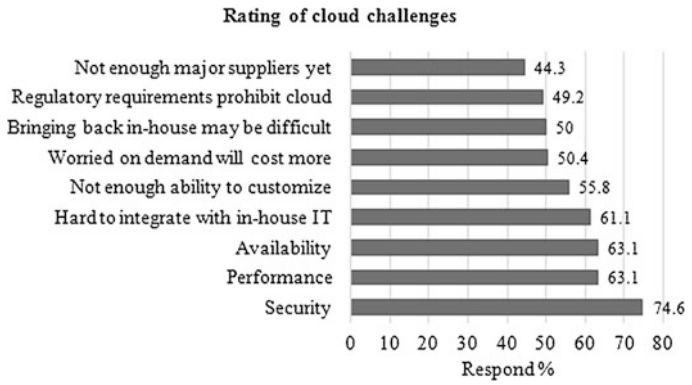

Fig. 2 Ranking of cloud environment challenges

The important problem on the cloud is data integrity. The confidential information stored in the cloud storage may suffer from harm or damage during transition actions from or to the cloud service provider such as the recently assaulted Linux's servers [8, 9].

Recent approaches for preserving the privacy and secrecy of users information stored in the cloud storages mainly include cryptographic encryption method (HMAC). Proof of Retrievability (POR) [10] is cryptography method for remotely checking the data integrity and confidential information stored on the cloud server. Information confidentiality and validity of data can be assured through cryptographic methods.

Bernd et al. [11] investigate vulnerabilities that are also a major security concern in a cloud. The control issue is a matter of vulnerabilities, which explore two examples as listed below:

- Virtualized networks offer inadequate network-based controls.
- Poor key management events

There are several areas of risks that could be identified, in which data and information security was the rate by 91.7% [12] as exposed in Table 1.

Table 1 Risk divisions with respect to cloud

Areas of risk	Critical (%)	Important (%)	Not so important (%)
Data and information security	91.7	8.3	0.0
Change control management	41.7	50.0	8.3
Third-party authentication management	41.7	41.7	16.7
Service-level agreement, regulations, and legislation	33.3	41.7	25.0
Disaster recovery	66.7	33.3	0.0

Some of the major cloud computing issues and different attacks [13] are mentioned below:

- Data confidentiality
- Vulnerability
- Leakage and loss of control
- Insider threats and malicious attacks
- Data intrusion
- Service hijacking
- Availability
- Hypervisor viruses
- Injection attack
- Denial of service
- Man-in-the-middle attack
- IP spoofing

3 Advanced Dynamic Authentic Security Method for Cloud Computing

The advanced dynamic authentic security method for cloud computing assesses the problem of security and privacy from the cloud architecture standpoint, cloud delivery model, and cloud deployment model perspective. This method appraises the problem of various attacks, data integrity, data leakage, information privacy, confidentiality, and vulnerability during the sharing of resources in cloud computing. It prevents scam, error, misuse of illegal access and rights in cloud computing environment. Cloud environment allows authenticated and authorized users' to access the confidential information and sharing of resources, which leads to developing effective and efficient security framework in the cloud computing environment. The need of filtering is enforced on the secure communication channel between cloud service provider and cloud user. To construct the self-directed security of protected cloud environment through an alliance with safety services such as authentication, privacy, and confidentiality.

To make sure of allocation of distribution information and availability of service by integrating cryptographic encryption method and protective sharing algorithm with authentication method [14]. This method strengthens the security which helps to control privileged user access and monitor activities of malicious users in a cloud environment. The advanced dynamic authentic security model for cloud computing is shown in Fig. 3.

This model applied a layered protective structure with different layers and ensures information security, eliminate various attacks, vulnerable file in this cloud environment.

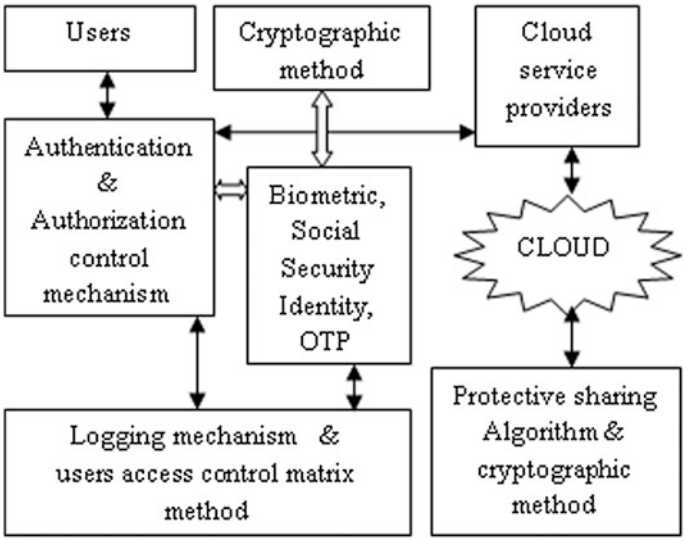

Fig. 3 An advanced dynamic authentic security model

The authentication and audit control method layer enforces user identity and validation mechanism through biometric authentic signature verification of users, one-time password method via mobile-based access security, social security identity card like Aadhaar card and separate user secret key. It controls and eliminates malicious users, attachers, and hackers with the help of centralized logging mechanism.

This dynamic security method also manages user access permission matrix method and keeps track of user activities via logging mechanism. This protective cloud computing environment provides an integrated extensive variety security solution, which ensures information confidentiality and data integrity.

In this method, protective sharing algorithm together with cryptographic methods to develop protective and sharing of resources and information in cloud computing environment [14]. The advanced dynamic authentic security model adopts multidimensional security architecture in cloud computing environment.

4 Performance and Evaluation

It is noticeable that a huge number of attacks like cross-scripting attacks, phishing attacks, threats are crashed the confidential data or reducing size, retreating sharing of services and resources, that would further enlarge the computational and communication expenses of improving services in cloud environment. The experimental results and analysis of the advanced dynamic authentic security method for

reducing various vulnerabilities, attacks in cloud computing environment have been described as follows.

The main aim is to reduce various attacks, threats, and vulnerabilities in cloud computing and it should maintain expenditure and standard consistent precision, which leads to develop and improve the high performance of cloud security systems.

Figure 4 shows that better audit frequency can be achieved throughout entire audit cycle by the sampling-based audit, which eliminates the load on the cloud servers and different attacks, raise the audit effectiveness under different detection probabilities on proportion of uncertain blocks in the whole file blocks. It supports a complete integrity verification and reduces computational and communication expenses of an audit service.

Figure 5 shows the time cost to select the peak-*k* resources or vulnerable documents on various sizes among set of resources through top-*k* select algorithm [15]. For example, it costs 1 ms to select the peak-500 resources or vulnerable files from a huge deposit of 1000 resources, while it costs 5 ms for the peak-1000 from 5000 resources or vulnerable files. Even though the cost of time is less, there is space for the decrease in case of huge *k*.

Figure 6 depicts that the time with respect to the cost of this point is autonomous to the quantity of enquired words on single or various resources or possible vulnerable files.

In order to decrease attacks, vulnerability, risk, threats in a cloud environment of any organization, present advanced dynamic authentic security method exploits better and is highly secure to safeguard the information, sharing of services and resources in the cloud environment. This method still guarantees practical competence with better performance while system robustness and security are notably improved.

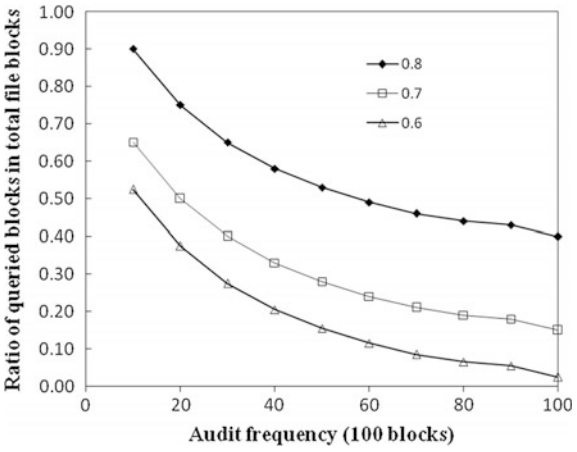

Fig. 4 Audit frequency with respect to proportion of uncertain blocks in the whole file blocks is shown

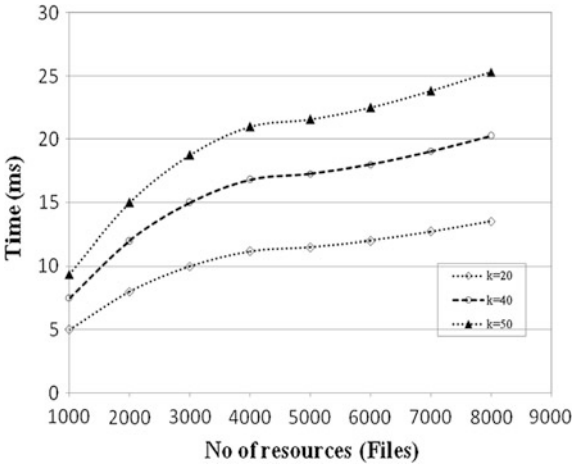

Fig. 5 The time required to select the peak-*k* resources or vulnerable documents on different resource sets is shown

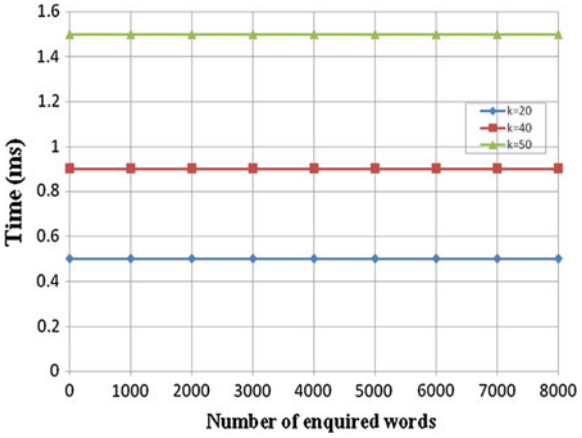

Fig. 6 The time needed to select the peak-*k* resources or vulnerable documents for several quantities of enquired words is shown

5 Conclusion and Future Work

Obviously, the present growth of cloud computing has quickly increased day-by-day, but cloud attacks, security, and privacy are still measured and it has been the most important key concern in the cloud computing. To protect confidential information and sharing of services and resources in cloud environment against threats and vulnerability a safer cloud environment is required, and therefore a suitable advanced dynamic authentic security is proposed for cloud technique and it should be enforced. This paper deals various security risks and challenges in terms of privacy, data intrusion, data integrity, data leakage, and confidentiality of cloud environment. This paper verifies user authentication and authorization management and keeps track of user activities through logging mechanism. This

paper proposes a strong dynamic security structure for cloud environment with many safety features such as shielding sharing of resources through cryptographic encryption mechanism with authentication techniques.

Future research on this work will include to develop a better auditing technique with specific standard interfaces and protocols that can maintain high confidentiality, security, integrity, and to meet more secure protected cloud environment.

References

1. Lin G (2012) Research on electronic data security strategy based on cloud computing. In: 2012 IEEE second international conference on consumer electronics, ISBN: 978-1-4577-1415-3, pp 1228–1231
2. Behl A, Behl K (2012) An analysis of cloud computing security issues. In: 2012 IEEE proceedings world congress on information and communication technologies, ISBN: 978-1-4673-4805-8, pp 109–114
3. Uma S, Kanika L, Manish M (2011) Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing. In: 2010 IEEE 1st international conference on parallel, distributed and grid computing (PDGC—2010), ISBN: 978-1-4244-7674-9, pp 211–216
4. Behl A (2011) Emerging security challenges in cloud computing. In: 2011 IEEE, ISBN: 978-1-4673-0126-8, pp 217–222
5. Chen D, Zhao H (2012) Data security and privacy protection issues in cloud computing. In: 2012 IEEE proceedings of international conference on computer science and electronics engineering, ISBN: 978-0-7695-4647-6, pp 647–651
6. Garfinkel SL (2007) An evaluation of amazon's grid computing services: EC2, S3, and SQS. Technical Report TR-08-07, Computer Science Group, Harvard University, Citeseer, pp 1–15
7. Zhou M, Zhang R, Xie W, Qian W, Zhou A (2010) Security and privacy in cloud computing: a survey. In: 2010 proceedings of sixth international conference on semantics, knowledge and grids, ISBN: 978-0-7695-4189-1, pp 105–112, 2010 IEEE
8. Cachin C, Keidar I, Shraer A (2009) Trusting the cloud. ACM SIGACT News 40:81–86
9. RedHat. https://rhn.redhat.com/errata/RHSA-2008-0855.html
10. Xu J, Chang E-C, Towards Efficient Proofs of Retrievability in Cloud Storage, National University of Singapore Department of Computer Science
11. Bernd G, Tobias (2011) Understanding cloud computing vulnerabilities. In: Co published by IEEE computer and reliabilities societies, IEEE April 2011, pp 50–57
12. Carroll M, van der Merwe A, Kotz P (2011) Secure cloud computing benefits, risks and controls. In: 2011 IEEE
13. Denz R, Taylor S (2013) A survey on securing the virtual cloud. J Cloud Comput Adv Syst Appl 2:17
14. Srinivasan S, Raja K (2014) Security challenges in cloud computing. Int J Emerg Technol Adv Eng 4(4):01–06, ISSN 2250–2459
15. Yu J, Lu P, Zhu Y, Xue G, Li M (2013) Towards secure multikeyword top-*k* retrieval over encrypted cloud data. In: IEEE Trans Dependable Secure Comput 10(4):239–250. July/August 2013

Author Biographies

S. Srinivasan is currently pursuing research at the Bharathiar University, Coimbatore, Tamil Nadu, India and is also working as Associate Professor at KCG College of Technology, Tamil Nadu, India. He received MCA from Bharathidasan University, India, in 1997 and M.E. from Sathyabama University, India, in 2009. His research interests include cloud computing. He is a member of CSI, ISTE, and IAENG.

K. Raja received Ph.D. from Sathyabama University, India, in 2006 and M.E. from Madras University, India, in 2001. Presently, he is the Principal and Dean (Academics) at Alpha College of Engineering, Tamil Nadu, India. He is a member of CSI, IEEE, ISTE, IETE, and IAENG. He has published in 25 international journals, 3 national journals, and 54 national and international conferences. He is a reviewer for national and international journals. His research interests include cloud computing and knowledge management.