Library Progress International
Vol.44, No.4, Jul-Dec 2024: P. 381-385

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Ensuring and Enhancing Security in the Realm of Cloud Computing

Vanshika Rathi, Shriniwas Singh

Research Scholar
Deptt. of M.Tech. C.S.E. Bharat Institute of Technology, Meerut
, Professor
Deptt. of C.S.E. Bharat Institute of Technology, Meerut
Email – vanshikarathi2738@gmail.com Shri0123@gmail.com

How to cite this article: Vanshika Rathi, Shriniwas Singh (2024). "Ensuring and Enhancing Security in the Realm of Cloud Computing". *Library Progress International,* 44(4), 381-385

Abstract

Because it allows users to access resources whenever they need them, cloud computing has completely changed the way organizations run. With the advent of the Internet of Things (IoT), a new paradigm for collaborative computing has emerged. The IoT relies on sensors and devices that produce and analyze massive volumes of data. This poses problems with scalability and security, heightening the importance of traditional security measures. So, to enable multi-user systems and facilitate simultaneous access to cloud resources by multiple users, we propose a novel Scalable and Secure Cloud Architecture (SSCA) in this paperThese findings demonstrate the efficacy of the proposed system. Similarly, SSCA outperformed the MHE-IS-CPMT, EAM, SCSS, and SHCEF models in terms of area under the curve (AUC), with improvements of6.30%,6.90%,7.60%, and 7.30% at the 25-user level and remarkable gains of 5.20%, 9.30%, 11.50%, and 15.40% at the 50-user level, respectively.

IndexTerms: Internet of Things, Cloud computing, Secure Cloud Architecture, Multicast and Broadcast Rekeying Algorithm, Post Quantum Cryptography

Introduction

The introduction of ARPANET, a network that facilitated the connection and exchange of information amongst a collection of computers [86], ultimately led to the creation of the Internet, which greatly simplified the process of linking different computer systems. The Internet has expedited several activities, including human contact via social media and instant messaging, as well as fulfilling the commercial requirements of organizations, such as online purchasing and financial services

The power, versatility, and user-friendly nature of CC are accompanied by several security issues. Despite CC being a novel and user-friendly method for accessing apps and streamlining work processes, there are some obstacles and concerns that might hinder its adoption. An incomplete investigation in this domain uncovers some problems. The key considerations include "Service Level Agreements (SLA)", the scope of migration, security measures, and more. CC has an automatic update capability, allowing any changes made by an administrator to a program to be immediately applied to all users. This posing a significant threat to organizations with limited security measures. Many academics also "cloud computing. Security" is the top-ranked problem in the field of CC .

Despite a company's claim of having top-notch security, if it fails to regularly update its security rules, it will become vulnerable to security breaches in the near future. Through this comprehensive research, we want to inform readers about several categories of security concerns and their corresponding solutions.

Literature Review

The author's name is A.M. Tjoa. Huemer and I investigate the privacy issue by empowering the end user with data control, hence increasing trust. The paper examines several Cloud computing threats and presents some strategies to mitigate these assaults [8][9].

Being knowledgeable and skilled in the various services available can aid in making an educated choice [8]. Companies must possess a thorough understanding of the various options and operational methods in order to effectively govern and manage data in the cloud. Cloud-based storage enables organizations to efficiently and flexibly store data at a reasonable cost [9, 10]. Efficiently managing data from its creation to its deletion is vital in cloud-based systems, highlighting the need of information governance for businesses. This involves the development of procedures for the storage, retrieval, and deletion of data, while also ensuring that data is sufficiently protected and secured against unauthorized access [11, 13].

Virtualization is an essential component of cloud computing that facilitates the delivery of the fundamental principles of cloud computing. Nevertheless, virtualization presents some hazards to data in cloud computing. An inherent danger is the potential compromise of a hypervisor itself.

If a hypervisor has vulnerabilities, it might be a major target. If a hypervisor is penetrated, it may lead to the vulnerability of the whole system, resulting in the potential compromise of data [11]. Another potential hazard of virtualization is linked to the allocation and deallocation of resources. If the VM operation data is not deleted from memory before reallocating it to the next VM, there is a risk of exposing the data to the next VM, which might be undesired [12]. An effective remedy for the aforementioned problems is to implement more strategic planning. Efficient use of resources and thorough authentication of data are essential before deallocating resources.

Methodology

PQC encryption, or Post-Quantum Cryptography encryption, is used to safeguard the communication material while it is being sent between many users and cloud servers [52].

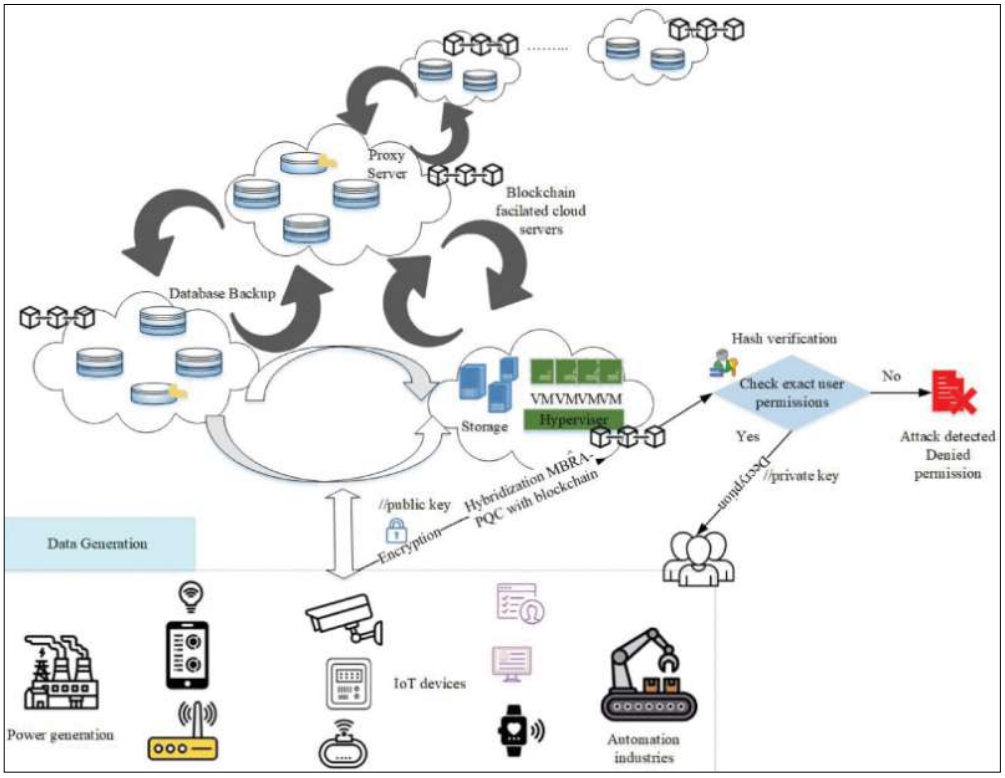

Fig. 1.2: Visual depiction presenting the proposed scalable and secure architecture.

Access management refers to the process of controlling and monitoring user access to various resources and functions inside a cloud platform. Its purpose is to prevent unwanted acts and maintain data confidentiality. This strategic integration greatly enhances its ability to accurately detect and proactively handle possible security risks, hence strengthening its resistance against different types of assaults. Access control refers to the processes that manage the rights and privileges given to users.

The proposed "Secure and Scalable Cryptographic Authentication (SSCA)" system is based on a hybridized "Multi-Blockchain Resilient Authentication (MBRA)" system, which incorporates a Blockchain and cryptosystem "Post-Quantum Cryptography (PQC)". This cryptosystem acts as the central security mechanism [52]. The hybridized cryptosystem, formed by integrating "Post-Quantum Cryptography (PQC)" and "Multi-Bit Rate Authentication (MBRA)" with blockchain technique, establishes a robust basis for ensuring secure communication inside the cloud system. This technology guarantees the privacy of sensitive data while it is being sent and provides defense against any assaults, providing a strong degree of security for both the system and the data it manages [53]. The next part explores the detailed methodology and formulation of the MBRA for detecting possible threats.

Preprocessing

Preprocessing steps include resizing images to a uniform size, normalizing pixel values, and augmenting the dataset with transformations such as rotation, scaling, and flipping. These steps enhance the robustness of the models.

Model Selection

Several ML and DNN models were selected for evaluation, including SVM, k-NN, RF, and CNN. These models were chosen based on their proven effectiveness in previous studies.

The models were trained on the preprocessed dataset using a stratified k-fold cross-validation technique to ensure robust evaluation. Performance metrics such as accuracy, precision, recall, and F1-score were calculated to compare the models.

Results

System security assessment entails analyzing vulnerabilities and evaluating the efficacy of established security measures in minimizing possible attacks. Ensuring the security of the system relies heavily on important factors such as effective management of cryptographic keys. By using this equation, anyone may accurately assess and compare the security efficacy of various models in a quantitative manner.

The equation Φ is defined as the cross product of x, the matrix P, and y, added to the summation of δ from t=0. The notation P[⋯] denotes the chance of security events happening. The equation presented offers a thorough framework for evaluating the degree of security in a system. It takes into account factors such as the probability, seriousness, vulnerability, and speed of reaction to possible security incidents. Through the assessment of these elements, individuals may get valuable information about the efficiency of the security measures and pinpoint areas that need improvement in the system's security.

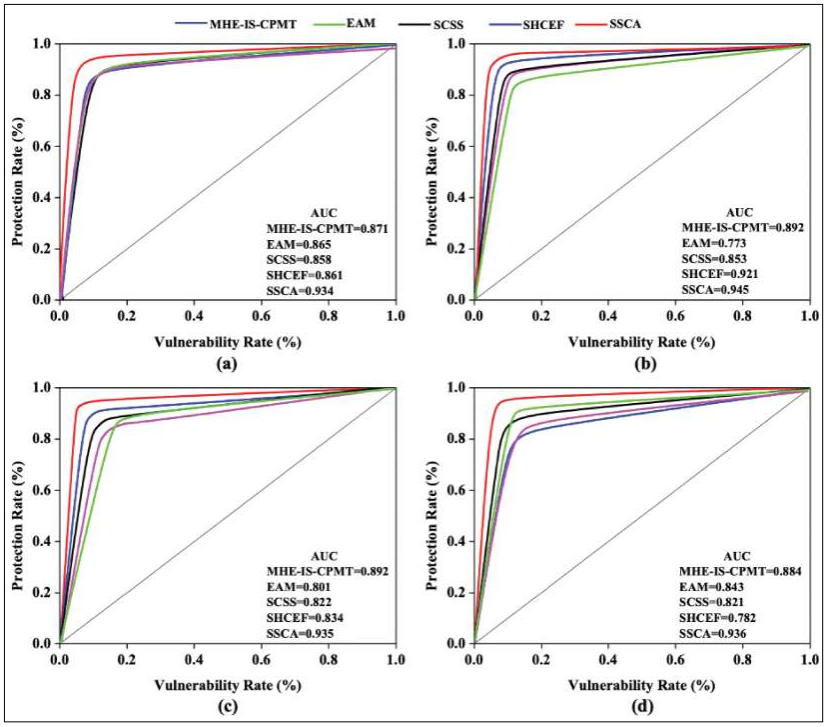

Fig. 4.2: Comparison of security by applying AUC

Moreover, with the growth in the number of users, all models likewise rise, suggesting enhanced security performance. Nevertheless, the SSCA model regularly demonstrates superior AUC values in comparison to the current models across various user levels.

Dependability

Reliability refers to the level of reliability shown by a system. It is often quantified as a percentage, signifying the extent of system downtime caused by security events or assaults. Reliability refers to the frequency at which a system maintains its usual functioning without experiencing any malfunctions during a certain period. The calculation of dependability may be calculated using equation (11). As a result of assault repercussions, as indicated by Equation (12).

The equation ϕ is equal to the product of φ and ξ(12).

"Let ϕ represent the frequency of system failures caused by attack consequences, φ represent the number of system failures caused by attack consequences, and ξ represent the total length of system uptime."

"We assess the dependability (R) and the occurrence of system failures caused by attack consequences (ϕ) for various values of system uptime (U) by graphing the length of system uptime on the y-axis and the rate of system failures owing to assault consequences on the x-axis. This enables us to evaluate the system's durability over some time."

Fig. 4.3 presents a comparison of the reliability metrics for 10 events among the current models SSCA, SHCEF, SCSS, EAM, and MHE-IS-CPMT. The most dependable model in this comparison is determined by identifying the model with the lowest percentage on the X-axis and the greatest % on the Y-axis. It exhibits enhanced resistance to assaults and quicker restoration from system failures induced by attacks, resulting in reduced occurrences of downtime.

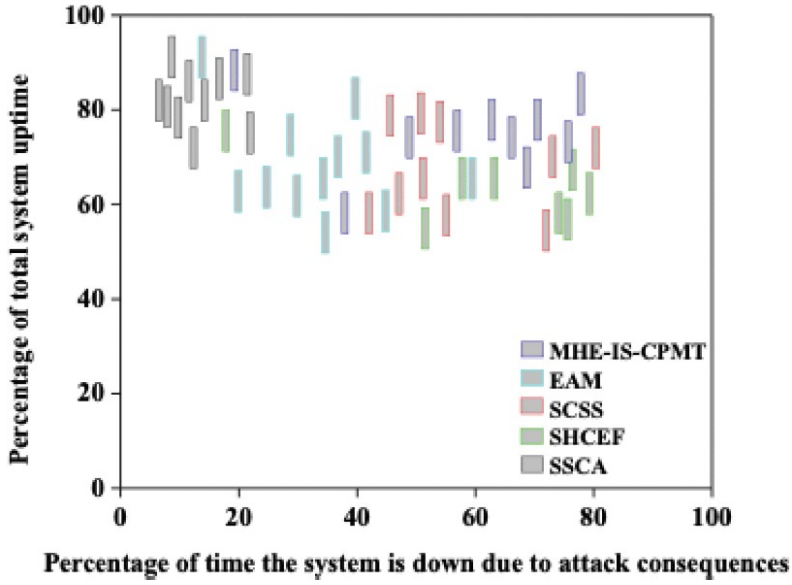

Fig. 4.3 presents a comparison of the dependability with the SCSS, EAM, and MHE-IS-CPMT techniques

CONCLUSION AND FUTURE WORK"

This study presents the Scalable and Secure Cloud Architecture, a new cloud architecture that incorporates IoT technology to efficiently tackle the complex concerns of data management, scalability, and security, in cloud computing. The suggested framework integrates decentralized cloud nodes, resilient MBRA & PQC encryption algorithms, and blockchain technology to guarantee efficient management of user requests, safeguard user information privacy, and assure secure storage of sensitive data. The architecture was purposefully built and meticulously tested to efficiently manage large data volumes and demanding situations. The assessment findings clearly show that the suggested SSCA outperformed current techniques, in terms of response time, scalability, and better security. More precisely, while analyzing the reaction times for 250 and 1000 devices, the MHE-IS-CPMT model showed response times of 7.69 and 9.19 seconds, whereas the suggested SSCA model demonstrated much better response times of 6.02 and 8.22 seconds, respectively. The SSCA demonstrates a significant improvement in reaction time, with a reduction of 1.67 and 0.97 seconds compared to MHE-IS-CPMT. In addition, when considering 25 users, the normalized AUC value for SSCA was 0.934, whereas the normalized AUC values for MHE-IS-CPMT, EAM, SCSS, and SHCEF were 0.871, 0.865, 0.858, and 0.861, respectively. At the 50-user level, SSCA obtained a normalized AUC value of 0.936. In comparison, MHE-IS-CPMT, EAM, SCSS, and SHCEF achieved normalized AUC values of 0.884, 0.843, 0.821, and 0.782, respectively. The findings indicate that SSCA performed better than other models, increasing AUC values by 6.30%, 6.90%, 7.60%, and 7.30% for the 25-user level, and 5.20%, 9.30%, 11.50%, and 15.40% for the 50-user level compared to the MHE-IS-CPMT, EAM, SCSS, and SHCEF models, respectively.

This future path seeks to evaluate the ability of SSCA to handle larger datasets and provide support for more intricate algorithms. Therefore, future improvements to SSCA will consist of including auto-scaling capabilities in addition to security methods and conducting thorough testing on a wide variety of datasets and user profiles to guarantee the delivery of cloud services.

REFERENCE

[1] A.Gutierrez,E.BoukramiandR.Lumsden, "Technologicalorganizationalandenvironmentalfactorsinfluencingmanagers'decisiontoadoptcloudcomputingintheU.K.",J.EnterpriseInf.Manage.,vol.28,no.6,pp.788-807,Oct.2015.

[2] A.Benlian,W.J.Kettinger,A.Sunyaev, andT.J.Winkler, "Specialsection:Thetransformativevalueofcloudcomputing:Adecouplingplatformizationandrecombinationtheoreticalframework",J.Manage.Inf.Syst.,vol.35, no. 3, pp. 719-739, Jul. 2018.

[3] X.Luo,S.ZhangandE.Litvinov, "Practicaldesignandimplementationofcloudcomputingforpowersystemplanningstudies",IEEETrans.SmartGrid,vol.10,no.2,pp.2301-2311,Mar.2019.

[4] A.El-Seoud,H.F.El-Sofany,M.Abdelfattah, andR.Mohamed, "Bigdataandcloudcomputing:Trendsandchallenges",Int.J.Interact.MobileTechnol.,vol.11,no.2,pp.1-19,2017.

[5] K.K.Patel,S.M.Patel, andP.Scholar, "InternetofThings-IoT:Definitioncharacteristicsarchitectureenablingtechnologiesapplication&futurechallenges",Int.J.Eng.Sci.Comput.,vol.6,no.5,pp.1-10,2016.

[6] S.N.Shirazi,A.Gouglidis,A.Farshad, andD.Hutchison, "Theextendedcloud:Reviewandanalysisofmobileedgecomputingandfogfromasecurityandresilienceperspective",IEEEJ.Sel.AreasCommun.,vol.35,no.11,pp.2586-2595,Nov.2017.

[7] B.H.Krishna,S.Kiran,G.Murali, andR.P.K.Reddy, "Securityissuesinservicemodelofcloudcomputingenvironment",Proc.Comput.Sci.,vol.87,pp.246-251,Jan.2016.

[8] D.Zeginis,F.D'Andria,S.Bocconi,J.G.Cruz,O.C.Martin,P.Gouvas,etal., "Auser-centricmulti-PaaSapplicationmanagementsolutionforhybridmulti-cloudscenarios",ScalableComput.Pract.Exp.,vol.14,no.1,pp.17-32,Apr.2013.