ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

A Survey on Various Security Techniques Used For Authentication

Akanksha Pal[1], Mayank Bhatt[2]

P.G. Student, Department of CSE, LNCTS (RIT), Indore, MP, India[1]

HOD, Department of CSE, LNCTS (RIT), Indore, MP, India [2]

ABSTRACT:Cloud computing is an emerging technology in the current time, but risks associated with this new technology and delivery model is not yet well understood. Because of the attractive features of cloud computing many organizations are using cloud storage for storing their critical information. The data can be stored remotely in the cloud by the users and can be accessed using thin clients as and when required. This technology provides services with one of the three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). This model allows users and organizations to share their vital information, crucial computing resources across the world. Securing these essential resources from the unauthorized access of the users is one of the major issues which lead to reduce the growth of this technology in the Information Technology (IT) Industries. Authentication is one of the major security parameters while providing access of the registered services to the intended users. In this paper we provide a survey on various cloud computing authentication techniques.

KEYWORDS:Cloud computing, security on cloud, hybrid cloud, authentication on cloud, cryptography.

I. INTRODUCTION

Cloud as defined by NIST [1]: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. Essential Characteristics:

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacentre). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

II. LITERATURE REVIEW

In this paper [2], authors had described a methodology of combining the keystroke analysis along with the existing authentication mechanisms to improve the security of delicate applications. They had explained their methodology with various references to be very effective and very efficient. Thus authors can ascertain the personal identity of the users even without their knowledge using keystroke analysis. The various limitations and the methods to overcome most of the limitations have also been mentioned. Thus, authors argue that their method can be used as a complementary or alternative way for user authentication and as an aid to intrusion detection to improve computer security.

In this paper [3], authors introduced an approach for allocating appropriate re-sources to advancement tasks so the execution may be completed which might satisfy objective functions such by users. It tries to enhance existing advancement scheduling algorithms that developed and deployed by numerous Grid Projects.

In this paper [4], authors introduced a new scheme which provide remote information integrity and verifiability means that dynamic information operations. The method first off identifies the difficulties and potential security issues of direct extensions with absolutely dynamic information updates. It achieves proficient information dynamics and improves the Retrievability model by manipulating the classic Merkle Hash Tree (MHT) construction used for block tag authentication. It's extremely proficient and secure technique.

Authors proposed an approach for planning and deploying end-to end secure and distributed software for the safety of information [5]. It guarantees that—above alittle trustworthy code base—data can't be leaked by buggy or malicious software parts. This can be crucial for cloud infrastructures, during which the keep information and hosted services all have totally different owners whose interests aren't aligned. It offers information tagging schemes and enforcement} techniques that may facilitate form the aforesaid trustworthy code base and cloud-hosted services that have end-to-end information flow control.

In this paper [6], authors proposed a new approach to instrument the cloud with hooks and supporting protocols and to develop mechanisms to extend mission-driven performance, resilience and security policies into the computing and communication infrastructure. By this approach twin problems with availableness and security within the cloud will be adequately self-addressed.

Authors proposed a design of micro-learning platform architecture made through cloud computing technology [7]; details the layered architecture design of micro-learning platform primarily based cloud, aiming at reckoning on the powerful computing capability and mass storage of cloud to better meet the sensible learning necessities of life-long learners.

In this paper [8] authors considered the Timing Covert Channel as a threat to network security, is exploited for identity authentication. Utilizing the packet intervals, authors implemented the TCC-based authentication on the common FTP platform. The authentication tag is embedded into thepacket intervals. The experiments show: 1) Their method is a secure way for authentication, since it is difficult to detect and decrypt the TCC authentication; 2) it could be implemented on many common network applications. In a word, the covert channel, such as TCC, can be a supplement for traditional authentication methods.

In this paper [9], an image authentication watermarking scheme based on image segmentation and sharing mechanism is proposed by authors. The scheme can resist VQ attack effectively because of the sensitiveness of segmentation algorithm. The authentication watermark can localize the alteration of the image contents, and the recovery data which are derived from different regions and embedded into the entire image, can almost restore the distorted regions effectively.

Authors introduced a handwriting authentication system [10]. The process allows secure access to restricted data in the cloud using a mobile phone. It is composed of pre-processing, feature extraction, classification and authentication process. The classification process is based on three different classification techniques: ANN, KNN, and Euclidean

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

Distance classifier. The classifier algorithm employs parallel combination of classifiers in order to achieve satisfactory accuracy on both recognition and error rate.

The combination of the cloud computing and mobile computing creates mobile cloud computing and also introduce security threats such as unauthorized users access. The authors focus in this research [11] is on the mobile cloud and protecting mobile cloud resources from illegitimate access. Biometric recognition will be used in the near future in mobile devices. The proposed solution by authors for authenticating mobile cloud users using the existing mobile device camera as a fingerprint sensor to obtain a fingerprint image, and then process it and recognize it. Results show that the proposed solution has added value to keep performance at an accepted level.

In this paper [12], authors propose a simple and effective online signature verification system that is suitable for user authentication on a mobile device. The benefits of the proposed algorithm are as follows. First, a histogram based feature set for representing an online signature can be derived in linear time and the system requires a small and fixed-size space to store the signature template. In addition, since the feature set represents only statistics about distribution of original online signature attributes, the transformation is non-invertible. As a result, the privacy of the original biometric data is well-protected. Second, a user-specific classifier comprising of a user-specific quantization step size vector and its associated quantized feature vector can be trained using only enrolment samples from that user without requiring a training set from a large number of users. Several experiments performed on MCYT and SUSIG datasets demonstrate effectiveness of the proposed method in terms of verification performance as compared to existing algorithms.

Security analysis of online signature verification system as compared to that of 4-digits PIN, and two usability metrics is also presented. Further investigation includes the use of other biometric key binding approaches, like fuzzy commitment, in order to strengthen security of the system, even when stored templates, helper data etc., are compromised, while preserving verification performance. Lastly, it is possible to derive a fusion approach by combining the proposed method with other existing approaches, e.g., DTW, HMM-based, etc., in order to improve verification performance, especially for applications where privacy of the signature traits is less critical.

In this paper [13], authors examine whether or not people could guess the hand-drawn images which were used as the graphical password of others, if they know some cultural information about the users, such as where they came from or their religion or even their hopes. The study also aims to contribute evidence of a bias in the user choice of images and considers the impact this could have on guessability. However, the results show that there is no difference between males and females and between members of different cultures in their ability to guess images. One clear result of this work is that it is apparently highly possible to guess other people's pass images if they contain cultural characteristics, especially religious marks, otherwise it is much more difficult to guess them. Also the authors provide Guidelines of drawing a secret password.

Authors proposed a Novel mutual authentication protocol for cloud computing using secret sharing and steganography in this paper [14]. The protocol is designed in such a way that it uses steganography as an additional encryption scheme. The scheme achieves authentication using secret sharing. Secret sharing allows a part of the secret to be kept in both sides which when combined becomes the complete secret. The secret contains information about both parties involved. Further, out of band authentication has been used which provides additional security.

According to the challenging issues during the userauthentication and access control process in cloud-basedenvironments, an efficient and scalable user authenticationscheme was proposed in this paper [15]. It the suggested model,various tools and techniques were introduced and used byusing the concept of agent. Therefore, a client-based userauthentication agent was introduced to confirm identity of theuser in client-side. Furthermore, a cloud-based software-as-a-serviceapplication was used to confirm the process ofauthentication for un-registered devices.

Moreover, there are two separate servers for storingauthentication and cryptography resources from main serversto decrease the dependency of user authentication andencryption processes from main server. Cryptography agentwas also introduced to encrypt resources before storing oncloud servers. In overall, the theoretical analysis of thesuggested scheme shows that, designing this userauthentication and access control model will enhance thereliability and rate of trust in cloud computing environments asan emerging and powerful technology in various industries.

In this paper [16], authors identified a new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is established to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users' access desires. Forward

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

security is realized by the session identifiers to prevent the session correlation. It indicates that the proposed scheme is possibly applied for privacy preservation in cloud applications.

In this paper [17], authorspresent a survey of recent trends to automatic recognition of human facial behaviour using soft computing. Soft computing is the most attractive field nowadays. Soft computing proves effective techniques to the problem of classification, prediction, optimization, pattern recognition, image processing, etc. The facial behaviour recognition processes in three steps in general. Face detection is the process of identifying face from images. Feature extraction is a process of highlighting the facial part that takes part in identification of expression and last a classifier is design that identifies the expression. There are a lot of effective methods are there to detect face expression, but no method performs best in all types of situation. Each method has their limitations. The future of human facial behaviour recognition system is to make a robust system that will perform efficiently in any circumstances.

Application developers may face with a adverse set of scenarios, each with its own identity solution without claim-based identity. Claim-based identity helps in providing a consistent answer across a wide range of scenario of cloud services. By building and deploying claim-based applications besides existing application result in simpler migration. Claim-based identity is not for only Microsoft vendors-many vendors are involved. In this paper [18], authors show why claim-based identity solutions are required and how to use by the cloud service provider in cloud applications.

III. CONCLUSION

In this paper we study various authentication techniques. Although there are various authentication schemes have been implemented for the security of these data but either they are too much complex or they require huge network resources. In most of the papers conventional password authentication schemes is used where server maintains password table or verification table which contains user identifier (ID) and password (PW) for all the registered users. It is used to authenticate the legitimate user.

In this survey most of the paper used one variable authentication. In the above review we have discussed various approaches based on cloud security.

REFERENCES

[1] Peter Mell,Timothy Grance , "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, 2011.
[2] Shiv Subramaniam K.N, Raj Bharath S, Ravinder S presented paper entitled "IMPROVED AUTHENTICATION MECHANISM USING KEYSTROKE ANALYSIS" at International Conference on Information and Communication Technology, ICICT 2007, 7-9 March 2007, Dhaka, Bangladesh.
[3] JiaYu, RajkumarBuyya and KotagiriRamamohanarao, "Workflow Scheduling Algorithms for Grid Computing", Metaheuristics for Scheduling in Distributed Computing Environments Studies in Computational Intelligence Volume 146, 2008, pp 173-214 @ Springer-Verlag Berlin Heidelberg.
[4] Qian Wang, Cong Wang, Jin Li, KuiRen, and Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", ESORICS'09 Proceedings of the 14th European conference on Research in computer security, Pages 355-370 Springer-Verlag Berlin, Heidelberg ©2009.
[5] Jean Bacon, David Evans, David M. Eyers, MatteoMigliavacca, Peter Pietzuch, and Brian Shand, "Enforcing End-to-end Application Security in the Cloud", Middleware '10 Proceedings of the ACM/IFIP/USENIX 11th International Conference on Middleware, Pages 293-312 Springer-Verlag Berlin, Heidelberg ©2010.
[6] Ravi Sandhu, Raj Boppana, Ram Krishnan, Jeff Reich, Todd Wolff and Josh Zachry," Towards a Discipline of Mission-Aware Cloud Computing". CCSW'10, October 8, 2010, ACM Chicago, Illinois, USA.
[7] Xiang Li, Jing Liu, Jun Han, Qian Zhang," The Architecture Design of Micro-Learning Platform Based on Cloud Computing", ICCC'11, August 13–14, 2011, ACM Wuhan, China.
[8] Yanan Sun, Xiaohong Guan, Ting Liu and Yu Qu presented paper entitled "An Identity Authentication Mechanism Based on Timing Covert Channel" at 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.
[9] Liu Yang, Rongrong Ni, Yao Zhao presented paper entitled "Segmentation-based Image Authentication and Recovery Scheme Using Reference Sharing Mechanism" at 2012 International Conference on Industrial Control and Electronics Engineering.
[10] F. Omr, S. FoufoU, R. HamiIa& M. Jarraya presented paper entitled "Cloud-based Mobile System for Biometrics Authentication" at IEEE 2013 13th International Conference on ITS Telecommunications (ITST).
[11] Iehab AL Rassan&HananAlShaher presented paper entitled "Securing Mobile Cloud Computing using Biometric Authentication (SMCBA)" at IEEE 2014 International Conference on Computational Science and Computational Intelligence.
[12] Napa Sae-Bae&NasirMemon presented paper entitled "Online Signature Verification on Mobile Devices" at IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

[13] Salem Jebriel& Dr. Ron Poet presented paper entitled "Exploring the Guessability of Hand Drawn Images Based on Cultural Characteristics" at IEEE 2014 6th International Conference on CSIT Published by the IEEE Computer Society.
[14] Nimmy K. and M. Sethumadhavan, "Novel Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography", 978-1-4799-2259-14/$31.00©2014 IEEE.
[15] FarazFatemiMoghaddam, Shiva GerayeliMoghaddam, SohrabRouzbeh, SaghebKohpayehAraghi, NimaMoradAlibeigi, ShirinDabbaghiVarnosfaderani, "**A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments**", 2014 IEEE Region 10 Symposium.
[16] Hong Liu, HuanshengNing, QingxuXiong& Laurence T. Yang presented paper entitled "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing" at IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 1, JANUARY 2015.
[17] KhyatiKantharia&Ghanshyam I Prajapati presented paper entitled "Facial Behavior Recognition using Soft Computing Techniques: A Survey" at IEEE 2015 Fifth International Conference on Advanced Computing & Communication Technologies.
[18] Ashish Singh &KakaliChatterjee presented paper entitled "Identity Management in Cloud computing Through Claim-Based Solution" at IEEE 2015 Fifth International Conference on Advanced Computing & Communication Technologies.