International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 3 Issue 1 January 2016

A Survey and Analysis of Various Cloud Computing Authentication Techniques

Atul Gupta[1], Prof. Shrirram Yadav[2]
PG Scholar CSE[1], PG Head CSE[2]
Millennium Institute of Technology, Bhopal
atul.gupta1112@gmail.com[1], techmillenniumk.yadav@gmail.com[2]

Abstract- *Cloud computing is a popular subject across the IT industry, there are lot of risks associated with this new technology. There are lots of attractive features of cloud computing that's why 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 & 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).Authentication is one of the major security parameters while providing access of the registered services to the intended users.*

Keywords—*cloud computing, security on cloud, hybrid cloud, authentication on cloud, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).*

1. INTRODUCTION

Cloud as defined by NIST [21]: 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 datacenter). 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.

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.

2. LITERATURE REVIEW

In this paper [1], a simple authentication technique for use in the GLOMONET has been proposed. This technique introduces a quite simple mechanism called “self-encryption” to simplify the authentication protocol. In the proposed authentication protocol, the temporary security manager in the visited network performs the same work that the original security manager in the home network does for regular communication. In other words, authors simplified the authentication protocol both for the roaming service and the regular communication. Thus, the complexity of mobile equipment can be decreased. Furthermore, the proposed technique reduces the number of transmissions during the authentication phase and, therefore, the requirement of the channel capacities has been reduced. On the other hand, authors also have proven that the self-encryption mechanism can be successfully adapted to another application in the mobility network, the secure teleconference service, to act as the authentication function.

In this paper [2], Authors had statistically analyzed inter-command time distributions between user commands and developed an analytic model that emulates statistical properties of the behaviors. They found that intercommand times were (in most cases) power-tail distributed. From this, they had demonstrated how probabilities of users executing a sequence of commands during a session can be ascertained. This was realized by developing an analytic model that incorporated both power-tail inter-command distribution times and auto correlated behaviors. Finally, via experimental results, they showed the efficacy of the new authentication mechanism by a series of experiments, which demonstrated that their methodology does indeed work.

In this paper [3], 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 [4], Authors had proposed a secure mutual authentication scheme for mobile communications based on a novel mechanism, i.e., nested one-time secrets. The proposed scheme given by authors can withstand the replay attack and the impersonating attack on mobile communications and it raises the performance of authentication. Compared with Hwang and Chang’s scheme, not only does the proposed scheme reduce the communication and computation cost of the entire protocol but also it reduces the cost required for the mobile users substantially.

In this paper [5], Authors had proposed a two-level distributed authentication architecture for wireless networks. Mobile hosts are using the Host Identity Protocol (HIP) to connect to the legacy Internet hosts through operator’s WLAN. The system includes an operator-specific proxy server and a distributed firewall running directly on WLAN APs. Authors had implemented the system by reflashing the firmware of two different AP models with Linux-based OpenWRT distribution.

In this paper [6], Authors had designed a system that uses a Bluetooth mobile device to unlock doors in a fully automatic process with the possibility to reconfigure the system to work in semi-automatic mode to get the approval of the user if he input a PIN code as additional security procedure. The design fulfills the requirement as defined with fast and secured distribution of the keys compared to the physical keys with minimum possible requirements for the hardware, reasonable power consumption and support for tailored personalized keys. An authentication protocol, a key distribution and a key revocation method were proposed.

In this paper [7] author states thatCoherent WSN security is not provided as long as the issue of initial trust between nodes is not fully addressed. This article introduces the concept of AVCA, a virtual certificate authority. It solves this issue of initial trust via the structured signing of certificates, which are implanted on devices prior to deployment.

Furthermore, AVCA supports node authentication and a private key distribution mechanism. It also enhances many WSN design goals including simplicity, scalability, interoperability and control for individual manufacturers. AVCA has been successfully implemented in a ZigBee protocol stack and can be easily incorporated into other WSN protocols. The authors are of the opinion that AVCA has the potential to offer a practical solution to many of the fundamental security issues that exist today with WSNs.

In this paper [8] authors had shown the drawbacks in the existing authentication protocol. This paper proposes to improve the performance Group Registration technique based on hybrid mechanisms is proposed in this paper. It results in lesser bandwidth consumption and reduces the computation and communication cost. The proposed scheme can withstand the replay attack and the impersonating attack on mobile communications. According to the analysis of authors it was proved that the proposed method is not only secure against various known attacks, but also more efficient than previously proposed schemes.

In this paper [9] 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 the packet 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 [10], an image authentication watermarking scheme based on image segmentation and sharing mechanism is proposed. 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.

In this paper [11] authors had designed and developed SPARSE on android based mobile phone to authenticate securely using Bluetooth on Remote system. Further they had evaluated cryptographic operations of IBE scheme. This scheme can be further explored to implement on different platforms and Key revocation problems can be explored in future. The implementation needs thorough security analysis to be carried out.

In this paper [12] authors states that Use of smart phones is increasing for application involving confidential data. They had developed a new tool for securing the information at rest in Android Platform that uses a lightweight authenticated encryption algorithm, Hummingbird-2, that is believed to be resistant to most of the standard attacks on block ciphers and stream ciphers. This tool protects the data at rest in android based smart phones thus providing security and confidentiality of stored data. Traditionally, pattern lock and password are the most widely used methods for authenticating the user. Their tool makes use of password based authentication But, password guessing can make the application vulnerable thus jeopardizing with the sensitive information.

In this paper [13] authors states that Magnus Kallus encryption scheme has tremendous potential, it can be combined with other encryption schemes such as RSA, DES, Diffie-Hellman Key Exchange, to make a new scheme for encryption. It may further be implemented for Digital Signatures. Other protocols can also be used for security of the keys like Diffie-Hellman Key Exchange or use a random number algorithm for generating the random numbers.

In this paper [14], Authors proposed a new software-efficient stream cipher with 128-bit key length. The proposed cipher implementation achieves competitive performance and sometimes better performance compared with the others. The complete diffusion requirement is satisfied after a single round. The influence of individual plaintext or key bits should spread over all the cipher text bits, so that the change in one plaintext or key bit causes the change of about 50% of the cipher text bits, uniformly distributed all along the ciphertext. The similarity of encryption and decryption means that in order to decrypt LEA cipher it is enough to repeat the same transformations performed throughout the encryption process.

In this paper [15] Authors had analyzed the utility of one of the most robust attacks against the simple substitution cipher when the ciphertext is obtained by the eavesdropper as the output of a symmetric discrete memoryless channel. The utility of the attack algorithm was presented as a function of channel mutual information in the case of noisy ciphertext, and the length of the observed ciphertext in the case of noise-free ciphertext. These two sets of results indicate an effective security gain that can be obtained if an eavesdropper can be made to observe only error-prone ciphertext, even for the simple substitution cipher. An example was presented to show how knowledge of the combined effect of cipherlength and channel noise can be used to determine the key agreement period of a substitution cipher cryptosystem.

In this paper [16] Authors states that after researching on IPv6 security, it is clear that much of IPsec vulnerability is based on DH exchange. The S-wane model mitigates this vulnerability by encrypting the DH exchange. This mechanism consists of a combination of RSA and DH and reduces considerably the vulnerability of AS negotiation security system. Therefore, replacing DH by Swane at this level enables the encryption of the information exchanged.

Moreover, Author's process helps to avoid the interception of conveyed data.

In this paper [17] Authors states the S-box is one of the major components in block cipher. Many methods generating the 4 x 4-bit S-box for the lightweight block cipher have been suggested in recent years. A common feature of these methods is using the Boolean minimization tool or simple nonlinear functions to obtain Look-Up Tables of the static S-box. Unlike the existing algorithm, the structure of dynamic 4 x 4-bit S-box based on chaos has been proposed. The 4 x 4-bit S-boxes in this study have fulfill the cryptographic properties of the "good" ones. The chaotic S-box chaining layer has more effective security than sBoxLayer of the current lightweight block ciphers. The chaotic S-boxes layer using the proposed chaotic 4 x 4-bit S-boxes has been implemented on the Altera DE2 FPGA, in which a small resource is required.

In this paper [18], a novel group key management scheme is proposed with perfect forward secrecy. The goal of this paper was to prevent from compromise of any key exchange among n-parties who shares a common secret over an insecure network. The Author States that any attacker can not reveal the short term group key even if the long term keys are accidently leaked or compromised. The scheme proposed by authors uses simpler steps and needs comparatively less communication and computation costs. According to the paper the security of the proposed scheme is based upon computational hard assumptions such as, Discrete Logarithm Problem (DLP) and Computational Diffie-Hellman Problem (CDHP). It is resilient against many key exchange attacks and provide Perfect Forward Secrecy using an ephemeral key. It works for large groups without delays in key generation and is observed under a trusted party.

In this paper [19] author has explained that some of the existing transposition techniques for creating a cipher text corresponding to the given plain text. Author has also given new technique for the encryption and decryption process is tested rigorously on different cases and verified results and found to be very correct and is working properly and it is able to encrypt and decrypt the plain text in the form of alphanumeric character, symbols, or any ASCII character without any loss of information and maintain the security of the message during the transmission over the network. Author has also determined that after preordering process for a 15 character size we can get it by 9 steps of preordering process (as 4 times in encryption process and 5 times in decryption process), the original data that was before preordering process.

In this paper [20] author proposed a scheme according to the challenging issues during the user authentication and access control process in cloud-based environments, an efficient and scalable user authentication. In the proposed scheme client-based user authentication agent was introduced to confirm identity of the user in client-side. Furthermore, a cloud-based software-as-a service application was used to confirm the process of authentication for un-registered devices.

In the proposed scheme two separate servers for storing authentication and cryptography resources from main servers to decrease the dependency of user authentication and encryption processes from main server. Cryptography agent was also introduced to encrypt resources before storing on cloud servers. In overall, the theoretical analysis of the suggested scheme shows that, designing this user authentication and access control model will enhance the reliability and rate of trust in cloud computing environments as an emerging and powerful technology in various industries.

3. PROBLEM IDENTIFICATION

Cloud providers offer cloud services to the consumer as per their demand with different benefits of cloud computing, like reducing run time and response time, minimize infrastructure risk, lower cost of entry, increased pace of innovation. Many security issues are coming with the cloud infrastructure which leads to impediment to the growth of cloud computing in the IT industries. 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. Objective to improve the data security in cloud computing based on advanced image authentication algorithm.

4. PROPOSED WORK

In conventional password authentication schemes, 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. Every user has an ID and PW. Whenever a user wants to access resources from a server, he or she submits ID and PW to pass the authentication phase. The server verifies the PW corresponding to the ID from verification table.

If the submitted password matches the one stored in the verification table then server authenticates the user. However, there is a threat in such a process; an intruder can impersonate a legal user by intercepting the messages from the network and login to the server later using the intercepted information. Even if the PW is encrypted during communication, such an impersonation attack is still possible. In addition, if an intruder break into the server; the contents of the verification table can be easily modified or stolen. Major downside of this scheme is securing the verification table which stores the password in plain text form. One of the solutions to cope up with this problem is to encode the password using hash function and store the resultant test pattern in a verification table. Another alternate solution is to store the password in encrypted form which cannot be easily derived from an attacker even if attacker knows the content of the verification table.

Introducing new concept using images will support a variety of the applications used by many associations, together with password management.

5. CONCLUSION

In this paper, we discussed various techniques that are implemented for authentication. Although there are various authentication schemes have been implemented for the security of cloud 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.A short survey of various cloud computing techniques and security authentication has been given also a brief about proposed work is mentioned.

6. SCOPE OF WORK

The solution for the above mentioned problems have a very vast scope. It can be applied in all areas where we use the conventional user Id & Password scheme. The areas where the solution can be applied are mentioned below-

- Web Portals
- Cloud Storage
- Hybrid Cloud
- Dynamic Servers

REFERENCE

[1]. Kuo-Feng Hwang and Chin-Chen Chang presented paper entitled “A Self-Encryption Mechanism for Authentication of Roaming and Teleconference Services” IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 2, NO. 2, MARCH 2003.

[2]. Craig Bossie & Pierre M. Fiorini presented paper entitled “A Dynamic Authentication Mechanism for Real-Time Network Security” at IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 5-7 September 2005, Sofia, Bulgaria.

[3]. 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.

[4]. Chun-I Fan, Pei-Hsiu Ho, and Hsin-Yu Chen presented paper entitled “Nested One-Time Secret Mechanisms for Fast Mutual Authentication in Mobile Communications” at IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings.

[5]. Dmitriy Kuptsov, Andrey Khurri, and Andrei Gurtov presented paper entitled “Distributed User Authentication in Wireless LANs” at IEEE in 2009.

[6]. Chia-Sheng Tsai and Cheng-I Hung presented paper entitled “An Enhanced Secure Mechanism of Access Control” at IEEE in 2010.

[7]. Edmond Holohan and Michael Schukat presented paper entitled “Authentication using Virtual Certificate Authorities” at IEEE in 2010 Ninth IEEE International Symposium on Network Computing and Applications.

[8]. Sridhar S and Vimala Devi.K presented paper entitled “Nested Mechanism for Mutual Authentication” at IEEE in 2011.

[9]. 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.

[10]. 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.

[11]. Shivraj V L, Rajan M A and Balamuralidhar P presented paper entitled “Secure Personal Authentication through Remote System for E- Transactions (SPARSE)” at IEEE in 2014.

[12]. Sushma Verma, Saibal Kumar Pal and S.K. Muttoo presented paper entitled “A New Tool for Lightweight Encryption on Android” at IEEE in 2014.

[13]. Vipul Srivastav presented paper entitled “New Approach in Encryption: Magnus Kallus” at IEEE 2014 International Conference on Computing for Sustainable Global Development (INDIACom).

[14]. Hadia M. El Hennawy, Alaa E. Omar and Salah M. Kholaif presented paper entitled “NEW PROPOSED STREAM CIPHER Algorithm” at 31st National Radio Science Conference, (NRSC2014), April 28 – 30, 2014, Faculty of Engineering, Ain Shams University, Egypt.

[15]. Nathan L. Gross and Willie K. Harrison presented paper entitled “An Analysis of an HMM-Based Attack on the Substitution Cipher with Error-Prone Ciphertext” at IEEE ICC 2014 - Communication and Information Systems Security Symposium.

[16]. Khadidiatou Wane Keita and Claude Lishou presented paper entitled “The Impact of Model S-Wane on IPv6” at IEEE in 2014.

[17]. Ta Thi Kim Hue, Thang Manh Hoang and Dat Tran presented paper entitled “Chaos-based S-box for Lightweight Block Cipher” at IEEE in 2014.

[18]. Susmita Mandal and Sujata Mohanty presented paper entitled “Multi-Party Key-Exchange with Perfect Forward Secrecy” at IEEE 2014 International Conference on Information Technology.

[19]. Nikhil Agrawal, Manoj Kumar and Dr. M.A. Rizvi presented paper entitled “Transposition Cryptography Algorithm using Tree Data Structure” at IEEE ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India.

[20]. Faraz Fatemi Moghaddam, Shiva Gerayeli Moghaddam, Sohrab Rouzbeh, Sagheb Kohpayeh Araghi, Nima Morad Alibeigi and Shirin Dabbaghi Varnosfaderani presented paper entitled “A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments” at 2014 IEEE Region 10 Symposium.

[21]. Peter Mell and Timothy Grance, “The NIST Definition of Cloud Computing”, NIST Special Publication 800-145, September 2011.