International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-2, December 2018

Client Authentication as a Service in Microsoft Azure

Harikrishna Bommala, S. Kiran, K. Mani Deep, Vadde Sunil Babu

Abstract*: *In today's Technological World, Information Security is an essential aspect for the internet applications. Cloud computing is an increasing current class of services for any type of users of the internet. In every modern technology like Cloud, authentication is very serious problem. So, many researchers apply various cryptography techniques to protect the sensitive data in the cloud systems. In this research work proposed on Client-Authentication-Verification Algorithm, Client–One-Time-Password-Authentication Algorithm, and Client - Authentication-Storage Algorithm for security and authentication in the cloud Model. These proposed algorithms have to provide strongest authentication mechanism to a cloud client. These techniques easily fit into any type of service in the cloud system.

Index Terms*: *Security, Authentication, Cryptography, Microsoft Azure Cloud.

I. INTRODUCTION

Cloud computing, as a new paradigm of information technology, has been developed the very quickly in recent years[1]. The widespread use of web-based Internet resources and the rapid growth of service providers have enabled cloud computing systems to become a model for large-scale IT services for networking distribute environments. Cloud system contains different deployment models like a public, private, community or hybrid [2]. The main elements of a cloud environment are abstraction and virtualization, which allows the technology to be perceived [3] and used in a completely different way than the existing legacy distributed systems[4]. The Major challenge issues to store the sensitive info in the cloud [13].

II. LITERATURE REVIEW

B.Harikrishna et al. Resource pooling on internet-based accessing on use as pay environmental technology and ruled in IT field is the cloud. Present, in every organization has trusted the web, however, the information must flow but not hold the data[5]. B. Harikrishna et al. When sensitive information is stored in the public welfare environment, problems arise when consumers leave the environment completely because they are not sure if the information is in the clouds [4]. Anyone who is trying to get the information from the cloud must be authorized by the service provider. It has multi ways to verify someone. Generally the user and password are utilized on multiple authenticated systems, but an unauthorized user can easily compromise. Validation is a big challenge when building internet security. In the cloud, password verification is the first level of security that only legitimate users should guarantee access to cloud data [6]. Multiform validation schemes provide more than one factor used to verify user information and then access data. The proposed procedure includes two true identity checks (2FA), which go beyond the various cloud security constraints and reduce costs [7]. It uses zero-level knowledge and unique password to validate two cloud-based factors. D. Ganesh Kumar and others proposed a new approach that provides cloud computing to determine the password. During the registration, the user provided all the information and stored it on the cloud server [13]. A user or server password can be created. After the registration process, the cloud user could access the cloud services through the login process. Protocol-based authentication and verification consisted of two modes [4]. User credentials were sent to the user's mobile devices. This procedure was used to avoid hacking of password and back-track attack using the generated password. With help of unique identification number, duos system possessed website. Mobile service provider involved during the password recovery phase [5]. This included two factors, that is, the password phase and the range of shots. Cloud users could easily change their password in the password change step and update the user's identity information in the cloud service environment [10]. For the resource to be sufficient, the identity can be at the device must first be checked, which is the authentication method before the authentication process [11]. The authentication processes, a mechanism of tracking mechanism must be used to record all successful and failed activities for authentication and application management [12].

III. MICROSOFT AZURE CLOUD

Windows Azure is the base for cloud applications and data. Instead of providing Microsoft customers with client software to install and use these computers, Windows Azure is a Windows service today: it uses customers to save and save applications for a Microsoft-owned machine. These applications can provide services to businesses, consumers, or both. Azure is a platform with in a flexible and interoperable to utilize for creating a new application [8].

Manuscript published on 30 December 2018.
***** Correspondence Author (s)
Harikrishna Bommala, Research Scholar, Department of Computer Science & Engineering, YSREC of Y.V University Proddatur, Kadapa (A.P.), India.
Dr. S. Kiran, Assistant Professor, Department of Computer Science & Engineering, YSREC of Y.V University Proddatur, Kadapa (A.P.), India.
K. Mani Deep, Assistant Professor, Department of Computer Science & Engineering, Bapatla Engineering College, Bapatla (A.P.), India.
Vadde Sunil Babu, Assistant Professor, Department of Computer Science & Engineering, IIIT Etcherla, Srikakulam, Etcherla (A.P.), India.

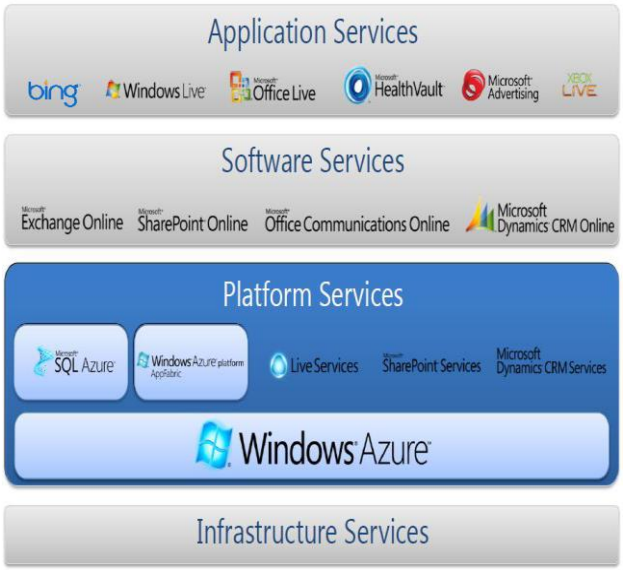

Fig 1: Microsoft Azure Cloud

Focus on developing applications run on Windows Azure entirely. Windows Azure platform is integrating with visual Studio. Azure is supports with Microsoft and non-Microsoft programming languages [8].

A. Azure Cloud Storage Services

Windows Azure Storage provides recurring and redundant cloud storage. "Microsoft's goal is to create a robust, secure, scalable, and efficient repository - Windows Azure Storage allows you to store data for a long time and store any amount of data [10].

Azure Queues: The messages between variation types of the application to create a secure network connection [7].

Azure files: Manage shared files for deployment on a cloud or on a site.

Azure Blobs: Extremely scalable storage element for binary and data.

Azure Tables: NoSQL store for schema without saving structured data [7].

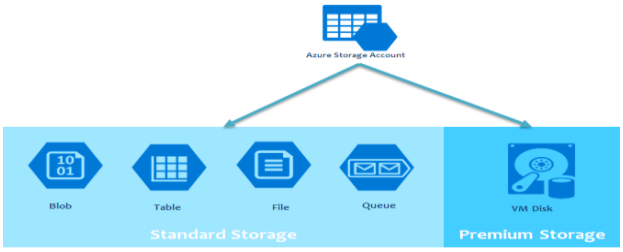

Fig 2: Windows Azure Storage Services

IV. PROBLEM STATEMENT AND MOTIVATIONS

Cloud computing offers on-pay as a service to provides a customers with the properties of distributed systems, like unlimited virtual resources, dynamic quantifiability, further as value advantages for business organizations. Real-time unauthorized access happens in Gmail, Yahoo and etc. the public cloud surroundings may be simply disclosed with various attacks from the unauthorized person from in and outside the cloud environment. Security problems that arise among this computing environment lead to various obstacles from each business and technological views. There's a continuous development of security solutions with a lot of challenges for a cloud environment. There are many existing authentication mechanisms that are not appropriate in different models during a cloud environment [8].

PaaS cloud security is considered one of many perspectives, including service provider access control, user protection, service continuity, and confidentiality. Authentication is compromised by various attacks like DoS, men-in-the-middle, brute force, etc[11]. It makes the large loss to the users once authentication is broken. As a solution to the present drawback, this work can investigate the way to manage authentication and authorization systems in cloud environments Authentication protects the entry of malicious attacks within the cloud. The transient study on the existing authentication mechanism was to conducted and located out that there's a desire for separate Client Authentication as a Service (CAaaS) in cloud computing. It's evident that an efficient authentication system doesn't compromise the opposite security parameters, like confidentiality, integrity and etc [10].

V. OBJECTIVE

The main scope of the objective work is Client-Authentication-as-a-Service (CAaaS) for the cloud to ensure to provide better security and authentication for sensitive data for the client.

- To determine authentication password generation algorithm for cloud security.
- To determine the Authentication by ensuring the valid cloud user to access the cloud service.
- To determine authentication verification generation algorithm for cloud security.
- To determine authentication secure data storage algorithm for text/image in the cloud.

VI. PROPOSED ALGORITHMS

CAaaS mechanism is provided as a separate service to cloud users. In this mechanism contains some different algorithms proposed like CAuth_OTP_G, CAuth_V, and CAuth_DataStorage. Initially, the User request to the new user and fill the details in application and submit their credentials. Once the user submits their credentials, CAuth_V generates a verification link is to be sent the registered user Email ID. After clicking the link it will be redirect to the login app in the browser. In the login page, the user will enter Email ID and password after submitting the details, by using the CAuth_OTP_G algorithm to generate a Otp will be sent to the registered Email ID [9]. After entering the Otp if the person is a valid user he/she will be consider to access the data in the cloud. The CAuth_DataStorage algorithm is to provide security for storing the images or Text in a cloud.

A. Algorithm for Client Authentication One Time Password (CAuth_OTP_G)

The CAuth_OTP_G algorithm performs to generate a strongest one-time password. The OTP includes alphanumerical values and special characters.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

By taken as input data is username and password, to utilizing the user credentials. These input values are converted into OTP using the different process, below mention algorithm is CAuth_OTP_G algorithm:

Start
step: 1 username+password
step 2: convert each character to ASCII value.
step 3: convert each ASCII value to binary format.
step 4: divide the binary values to even and odd positions-->even[]&&odd[]
step 5: perform xor operation on even and odd positions values-->xor[]
step 6: divide the xor[] into 8 values buffer array--->buffer[]
step 7: convert each value in buffer[] into a decimal number
step 8: based length convert each decimal number to Otp
stop

B. Client Authentication Verification (CAuth_V) algorithm

The CAuth_V algorithm is to implementing to used to verify the cloud, generated otp and enter otp are matched, then to access the cloud. If not matched to access denied to the cloud.

Algorithm for Client Authentication Verification (CAuth_V):

Start
Step 1: The client enter client name and password, and getting it.
Step 2: checking them with the client name and password in the database---->one factor is done
Step 3: input Otp from the user
Step 4: get generated Otp
Step 5: if input Otp===generated Otp---> two factors
Access to cloud
else
Access denied

C. Image and Text Storing In the Cloud Process Algorithm

Now by using to generate the otp and verify link to send register mail. Based upon the Otp and verify it, to create two tables i.e (imgtable and text-table) are in the cloud database. After completion of verification then, the client is able to store the image into imgtable and the text is stored in a text table.

CAuth_DataStorage algorithm:

1. Creating a key during the user registration
2. Based on the key two tables (imgtable, text-table) are designing in the cloud database
3. If the verification is done then the user will be able to consider and accessing to store the images into imgtable and the text into a text-table.

D. Implementation Proposed Algorithm with Microsoft Azure

Step 1: Create an account in windows azure free or pay as-use credentials.
Step 2: After creating an account in the Azure cloud than to install in local system in Visual Studio 2017, Windows Azure SDK and SQL Server 2008 R2Express.
Step 3: In windows azure hosted service control panel has a "new hosted service" click it and create the web application.
Step 4: In this work, to write an application code in a local system by using .Net frame work version for Visual Studio (VS) 2017 for Cloud project.
Step 5: In that application to add web role that is ASP MVC3.
Step 6: In locally application parallel to design a database in Management Studio in version 2008 of Microsoft SQL Server R2 Express.
Step 7: In Cloud Project has different name space created like CloudApplication.aspx, Login.aspx, MailVerification.aspx, OtpVerification.aspx RestPass.aspx admin.aspx, Default.aspx, Forget.aspx, and, which contains files with aspx.cs. The cloud project behind and inherits .cs files each one updated.
Step 8: The file of Web.config has contains two files Web.Release.config and Web.Debug.config. It file has to be updated of the application with the SQL Azure database connection string.
Step 9: Cloud project has to be deployment by requires package location (.cspkg) and configuration files (.cscfg).
Step 10: successfully deployment and build Cloud project in Azure Cloud.

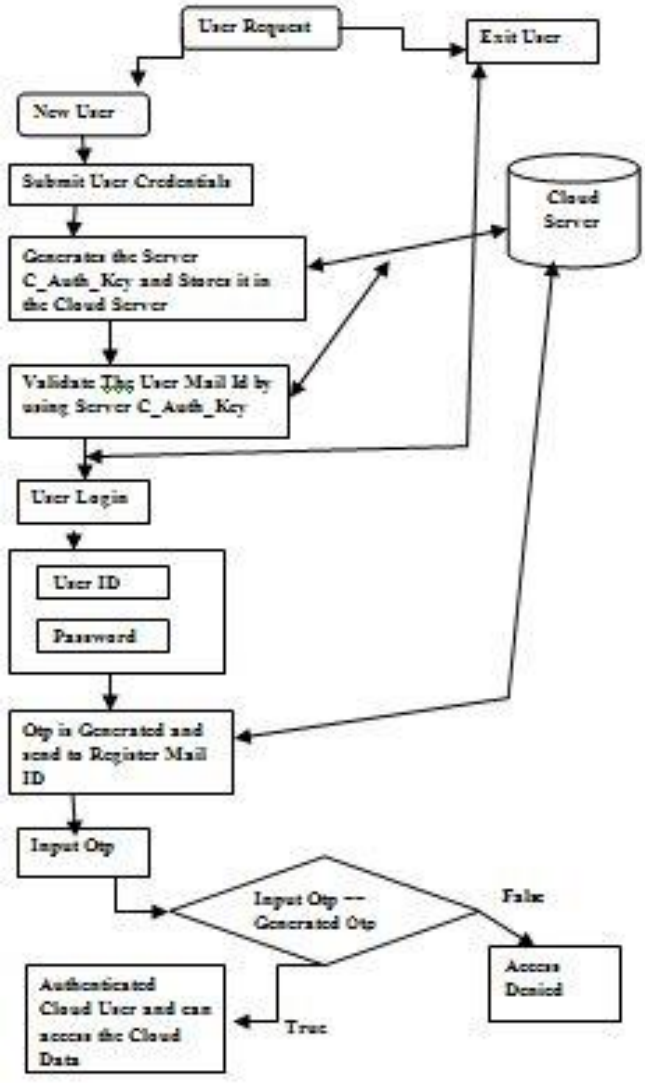

Fig: 3 Clients -Authentication as a Service

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

VII. EXPERIMENTAL RESULTS

Fig 4: Registration Form for Client

Fig 5: Verification has been sent to Mail Id and Verification Link

Fig 6: Client Mail Verified and Login

Fig 7: User gets the Otp from CSP

Fig 8: Enter Otp sent to Register Email Address and open Client Cloud Application

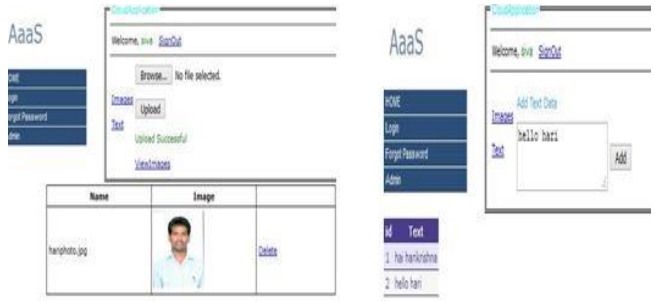

Fig 9: Client stores the Image and Text in Cloud Application.

VIII. CONCLUSION

The rapid development technology is a cloud computing. However, the security is major challenge issues in cloud computing. One of the major factors of cloud security challenge is Authentication. In every day increases major challenges are Security and Storage in the stream of a cloud. In research work, a CAaaS (Client Authentication as a Service) is proposed to the high secure algorithm for authentication by accessing the cloud. CAuth_OTP_G is used to produce the OTP and clients of the registered mail account to sent the otp. CAuth_V is used to generate a link to send clients register mail account and verify whether the client is a registered user. If the client is entering the login in the cloud, then verify in the database of the cloud both are same, the users can access the data in a cloud environment. The CAuth_DataStorage algorithm is performed to store the clients' sensitive info in the cloud.

REFERENCES

1. BH Krishna, S Kiran, G Murali, RPK Reddy "Security issues in service model of cloud computing environment" Procedia Computer Science, 2016, published Elsevier page no: 246-251, volume no 87.
2. https://azure.microsoft.com/en-in/tools/
3. Yu J, Wang G, Mu Y, Gao W. "An efficient generic framework for three-factor authentication with provably secure instantiation" IEEE Transactions on Information Forensics and Security. 2014; 9(12):1–12.
4. Harikrishna Bommala, Dr.S.kiran, RPK Reddy, K.Mani Deep, "Network as a Service Model in Cloud Authentication by HMAC Algorithm" Int. J. Advanced Networking and Applications Volume: 09 Issue: 06 Pages: 3623-3631 (2018) ISSN: 0975-0290.
5. B. Harikrishna, S. Kiran, R. Pradeep Kumar Reddy, "Protection on sensitive information in cloud Cryptography algorithms", IEEE digital Library 10.1109/CESYS.2016.7889894.
6. Lee S, Kim TY, Lee HJ. "Mutual authentication scheme for cloud computing" Future Information Communication Technology and Applications. 2013; 235:149–57.
7. Jiang R. "Advanced secure user authentication framework for cloud computing" International Journal of Smart Sensing and Intelligent Systems. 2013 Sep; 6(4):1700–24.
8. https://visualstudio.microsoft.com/vs/features/azure/
9. Harikrishna Bommala, "https://www. scholars-press.com/catalog/details/store/gb/book /978- 620 - 2-30024-7/computer-programming-in-c?search=978-6202300247"published date 2017/8/4.
10. Kataria S, Syal R. "Secure mutual authentication for cloud environment", International Journal of Computer Science Engineering and Technology. 2015 Jul; 5(7):214–18.
11. Jiang R. "Advanced secure user authentication framework for cloud computing" International Journal of Smart Sensing and Intelligent Systems. 2013 Sep; 6(4):1700–24.
12. Soni P, Sahoo M. Multi-factor authentication security framework in cloud computing. International Journal of Advanced Research in Computer Science and Software Engineering. 2015 Jan; 5(1):1065–71.
13. Kumar DG, Rajasekaran S, Prabu R. PB verification and authentication for server using multi communication. Indian Journal of Science and Technology. 2016 Feb; 9(5):1–6. DOI: 10.17485/ijst/2016/v9i5/87154.

AUTHOR PROFILE

Bommala Harikrishna, Currently pursuing as Full Time Ph.D Research scholar in Y.S.R E.C of Yogi Vemana University, Proddatur from the department of Computer Science & Engineering, under the guidance of Dr. S. Kiran, Assistant Professor, department of CSE. He is Former Lecturer and In-Charge coordinator of QEEE at JNTUA College of Engineering Pulivendula, Pulivendula, Kadapa, and A.P. And also Worked as Assistant Professor in A1 GLobal Institute of Engineering and Technology, Markapuram, AP.

He completed Master in Technology at Acharya Nagarjuna University, Guntur and Bachelor in Technology at JNTU Kakinada. He published twenty two international journals and conference. He published five National journals and conference. He is a member of SWIDC, ISTE, UACEE, IAENG, IJCSE, IJCSA and ITHISTORY. Interested research areas are Cloud Computing, Data Security in Cloud, Network Security, Data Structure, and Machine Learning with Cloud, IOT with Cloud Security, Information Security and Big Data Security.

Dr. S. Kiran is Assistant Professor in the stream of Computer Science and Engineering at Y.S.R E.C of Yogi Vemana University, Proddatur from Yogi Vemana University, Kadapa. He acquired M.Tech Degree from Nagarjuna University, Guntur. He completed Ph.D in Computer Science in from S. K. University. He has been continuously imparting his knowledge to several students in research activities. He published many articles National and International journals. He published thirty international journals and conference, seven International conference proceedings published in IEEE explore and one international conference proceeding published in SCIENCE Directory with Elsevier. He is a member of SWIDC, ISTE, UACEE, IAENG and IJCSE. His Interested research areas are image processing, Cryptography and Network Security, Genetic Algorithms, Software Engineering and Data Security in Cloud.

K. Mani Deep is Assistant Professor in the department of Computer Science and Engineering at Bapatla Engineering College, Bapatla. He completed Master in Technology at Acharya Nagarjuna University, Guntur and Bachelor in Technology at JNTU Kakinada. He has been continuously imparting his knowledge to several students in research activities. He published many articles National and International journals He is a member of SWIDC, UACEE and IAENG. His Interested research areas are Cloud Computing, Data Security in Cloud, Cryptography and Network Security, Machine Learning with Cloud and IOT with Cloud Security.

Vadde Sunil Babu is Assistant Professor in the department of Computer Science and Engineering at IIIT- Srikakulam. He completed Master in Technology and B.Tech at Acharya Nagarjuna University, Guntur. He has been continuously imparting his knowledge to several students in research activities. He published many articles National and International journals He is a member of SWIDC, UACEE and IAENG. His Interested research areas are Cloud Computing, Data Security in Cloud, Cryptography and Network Security, Machine Learning with Cloud and IOT with Cloud Security.