A Review Article on Authentication Protocols in Cloud Computing

Umaira Fatima¹ and Dr. Sheeba Parveen²
¹Student, Department of Computer Science & Engineering, Integral University, Lucknow, INDIA
²Associate Professor, Department of Computer Science & Engineering, Integral University, Lucknow, INDIA

Corresponding Author: umaima0112@gmail.com

ABSTRACT

Cloud computing technology provides on-demand computing resources like software, hardware and storage in pay-per-use model. Cloud computing is very beneficial for today’s organizations, as there is no need to maintain physical infrastructure. These services and resources can be accessed from anywhere anytime over the internet. It is cost effective as users only need to pay for resources they use. Many individuals and organizations have shifted themselves over cloud environment as it is cheaper and convenient. As huge amount of sensitive data is being stored and processing in cloud computing environment so there is major concern of security. Lack of security may cause several issues. It may result in loss of organisation’s data and may even leak confidential data of user and organisation to unwanted access. To implement security in cloud computing various authentication and encryption protocol exists. This aim of this paper is to review various authentication protocols given by various researchers all over the world.

Keywords-- Cloud Computing, Security Issues, Authentication, Authorization

I. INTRODUCTION

Cloud computing is providing on-demand services such as data storage, computing power, databases, software and servers over the internet. Cloud computing uses pay-per-use model. It allows to lower operational cost and scale business easily in times of need and lowers operational cost.

Cloud computing provides various advantages. It is being used in modern world in banking [1] and various other sectors[2][3][4]. It allows to easily scale resources and storage without investing in physical infrastructure. The user has to pay only for the resources that he actually use. Cloud computing allows to access data from anywhere anytime over the internet. Despite offering number of benefits, cloud computing suffers security challenges that must be addressed and taken care of.

A. Security Challenges of Cloud Computing

There are a lot of security challenges in cloud computing[5][6][7][8]. Researchers all over the world have analysed security issues and provided measure to improve it[9][10]. Cloud services faces various security issues[11]. Cloud service are vulnerable to denial of service attack that may result in downtime of entire system and halt the ongoing operation[12]. There are several insider threats in cloud computing such as Any malicious user gets into system access private and sensitive data. Many other attacks are also there in Cloud computing like Man-in-the-middle attack[13]. SQL injection attack[14] and various other attacks. There may be data breaching issue too if a cloud service provider does not provide adequate security measures which in turn may result in unauthorized access to data. Cloud services are exposed to various user interfaces and application programming interfaces (APIs). If security measures are not adequately enabled in APIs then a user who is not authorized may access data and may re-use the APIs or passwords.

B. Types of Cloud

1. Public Cloud: Public clouds are the cloud computing services available publicly over the internet that can be accessed by any authorize user in pay-per-use model. They are highly elastic and scalable. Public clouds are mostly managed and provided by some third party service providers. Public clouds provide a range of services such as computing power, storage, networking, and applications that are accessible over the internet, and can be quickly provisioned, scaled up or down, and accessed remotely from anywhere with an internet connection. Public clouds are known for their scalability, flexibility, and cost-effectiveness.

2. Private Cloud: The private clouds are dedicated for use of a particular organization. In private cloud organisations have complete control over resources, security and data. Private clouds are used by organisations that have more control over data and have specific security requirements or they have some sensitive data or work. Here computing resources and services are delivered via secure private network. It has less security issues as compared to public cloud.
3. Hybrid Cloud: Hybrid cloud services combine both public and private cloud solution. Here applications and data share resources between public and private cloud service based on requirement. Hybrid cloud allows flexibility and helps to meet demands in times of changing requirements of an organization or individuals in modern world [15][16][17].

4. Community Cloud: Community cloud service is a cloud service managed and used by a group of members or community for a special purpose. Community cloud is designed to serve the need of specific community with similar interests and requirements. It provides a way between public and private cloud offering a level of customization, security and privacy that may be required by organizations with shared interests. Community clouds are commonly used by organizations such as healthcare, government, finance, and education, where there are shared interests and requirements, or collaborative initiatives.

C. Cloud Computing Services

Various types of services are provided by cloud computing [18], some of them are as follows:

1. IaaS: Infrastructure as a service in this cloud service model resources and infrastructures are distributed as a service. It is highly scalable and flexible. Here highly scalable and automated [19]. Its infrastructure are rented to compensate the need of physical resources and workstations. Here large amount of sensitive data is being hosted so it is essential to ensure security. In [20] a framework is proposed that ensures security in IaaS.

2. PaaS: platform as a service [21]. It provides both hardware and software tools which are used by developers to build application and services. PaaS is very scalable cloud computing service. It suits different type of businesses according to resources. It provides the business organisations and individuals a complete development and deployment environment. The users purchase these resources as they need and access them over a secure internet connection.

3. SaaS: software as a service it allows software and its functions available in pay-per-use model. It is a service that hosts software to be available for users. SaaS is highly scalable cloud computing service. It suits small and medium level and enterprise level business. SaaS allows applications to run on SaaS providers’ server without installing them on local machine [22].

II. COMPARATIVE STUDY

Due to security risks and issue in cloud computing, there is a strong need of authentication and authorization in cloud computing. Various authentication techniques and protocols exist provided by researchers all over the world. This paper provides literature survey of various existing authentication protocols. A biometric based authentication scheme was given [23] to provide authentication of users based on elliptical key cryptography. In [24] a model was proposed that used the mathematical method to provide single server and two server Password based Authentication Systems. Further multi-level authentication was proposed in [25]. A three step security system was given in [26] that used steganography and cryptography techniques. In [27] an ECC based authentication technique was proposed that used digital signature based identification. A lightweight authentication method was proposed in [28] as most of the existing one had higher computation cost. A lightweight authentication system was also proposed in [29] based on message digest and location.

A multimodal based biometric authentication method was developed in [30], using fingerprint and iris.
### Table 1: Literature survey of various Authentication protocols in cloud computing

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Year</th>
<th>Author</th>
<th>Keywords</th>
<th>Proposed Method</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2023</td>
<td>Linsheng Yu[31]</td>
<td>blockchain, authentication, mobile cloud computing</td>
<td>Authentication and authorization based on blockchain</td>
<td>efficient and scalable. Enhanced security of the mobile cloud computing</td>
<td>High storage overhead</td>
</tr>
<tr>
<td>2</td>
<td>2022</td>
<td>Kaur.Sandeep [32]</td>
<td>a novel one way hash, two factor authentication</td>
<td>ID Password OTP based verification Encryption using RSA , ECC</td>
<td>Survived MITM attacks, brute force attack, Account and session hijacking attack, replay attacks,</td>
<td>Not covered man In the middle attack</td>
</tr>
<tr>
<td>3</td>
<td>2022</td>
<td>Tsu-Yang Wu[33]</td>
<td>Cloud computing, IOT, SGX, authentication</td>
<td>Intel software-guard-extensions based authentication protocol</td>
<td>reduce communication cost by 7.07% in comparison with best existing algorithm</td>
<td>Computational cost is higher slightly</td>
</tr>
<tr>
<td>4</td>
<td>2022</td>
<td>Syed Amma Sheik[34]</td>
<td>ANN , Authentication ,Cloud computing</td>
<td>Cryptography using ANN</td>
<td>Survived various Malicious Attack</td>
<td>Only ANN is not enough to provide security in cloud computing</td>
</tr>
<tr>
<td>5</td>
<td>2021</td>
<td>Diksha Rangwani1 [35]</td>
<td>Cloud computing, authentication, ECC</td>
<td>ECC and irreversible hash function</td>
<td>Robust against replay attack, Man in the middle attack ,nearly all attacks, lightweight</td>
<td>N/A</td>
</tr>
<tr>
<td>6</td>
<td>2020</td>
<td>Abdelrahman Abuarqoub [36]</td>
<td>smart card, Dual factor authentication , Mobile cloud computing</td>
<td>Smart card based password verification</td>
<td>successfully survived various insider and outsider attacks</td>
<td>can be improved further to be used in IOT and various other industries</td>
</tr>
<tr>
<td>7</td>
<td>2020</td>
<td>Feifei Wang[37]</td>
<td>Authentication, IOT</td>
<td>IoT-based three factor authentication</td>
<td>Achieves three factor secrecy and resilient to offline guessing, session key disclosure, replay and various other attacks</td>
<td>N/A</td>
</tr>
<tr>
<td>8</td>
<td>2019</td>
<td>Ghassan O. Karame, [38]</td>
<td>data confidentiality, Key exposure</td>
<td>Bastion, which offers data confidentiality even at time of</td>
<td>Very small overhead</td>
<td>Good security with high throughput</td>
</tr>
<tr>
<td>No.</td>
<td>Year</td>
<td>Author(s)</td>
<td>Field</td>
<td>Protocol</td>
<td>Security Features</td>
<td>Success Rate</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-----------</td>
<td>-------</td>
<td>----------</td>
<td>------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>9</td>
<td>2019</td>
<td>Rafael Martínez-Peláez [39]</td>
<td>Cloud computing, mutual authentication, IOT</td>
<td>IOT based authentication scheme J.R.P.M., R.M.P., V.G.L.J.M.</td>
<td>Better computation and communication cost, Overcome user impersonation and replay attack</td>
<td>N/A</td>
</tr>
<tr>
<td>10</td>
<td>2018</td>
<td>Mylara Reddy Chinnaiah et.al., [40]</td>
<td>Cloud security, risk and issue, authorization</td>
<td>Fault tolerance technique: Characteristics &amp; Frequency if interactions(ChIFrFT), Frequency of Configuration interactions(IFrFT)</td>
<td>Better than NOFT scheme achieves reliability and fault tolerance in cost efficient manner</td>
<td>Low successful interaction about(25-40%)</td>
</tr>
<tr>
<td>11</td>
<td>2017</td>
<td>Noelle Rakotondra vony et.al. [41]</td>
<td>VMI, Malware</td>
<td>VMI based malware analysis</td>
<td>Focused on invention of target and direction of attack</td>
<td>Listed issues but less focus on their solution</td>
</tr>
<tr>
<td>12</td>
<td>2016</td>
<td>Punam V.V.Maitri &amp; Aruna Verma Et.al. [42]</td>
<td>Stegnography, AES</td>
<td>LSB stegnography with use of RC6, AES, BRA algorithm</td>
<td>Tried to provide high level of security using hybridization of public key. Focused on data integrity and low delay</td>
<td>Not able to provide high level of security</td>
</tr>
<tr>
<td>13</td>
<td>2015</td>
<td>Primoz cigoj et.al., [43]</td>
<td>Authentication</td>
<td>Single sign on (SSO) approach</td>
<td>Secure and strong authentication</td>
<td>It needs more flexible interfaces, It attempt to remove some vulnerability only</td>
</tr>
<tr>
<td>14</td>
<td>2014</td>
<td>Nitin Nagar &amp; Pradeep K[44]</td>
<td>Authentication, LDAP</td>
<td>LDAP authentication</td>
<td>Provide a secure framework and helps in protection of user data</td>
<td>No focus on cloud computing tool for implementation</td>
</tr>
<tr>
<td>15</td>
<td>2013</td>
<td>Umer Khalid et.al., [45]</td>
<td>Authorization, Authentication</td>
<td>Anonymous Authentication &amp; Authorization</td>
<td>Survived identity theft, leakage of data and integrated with the existing systems of identity management</td>
<td>N/A</td>
</tr>
<tr>
<td>16</td>
<td>2013</td>
<td>Kok-Seng Wong [46]</td>
<td>Biometric based authentication, cloud, authentication system</td>
<td>Voice iris, fingerprint etc are taken as credential input for authentication</td>
<td>Secure against malicious user and service provider</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The above table shows Literature survey of various Authentication protocols in cloud computing.
III. RESULTS AND DISCUSSION

There are several research gaps in above authentication algorithms. 

**Standardization:** Any standardize protocol does not exist for authentication in cloud computing environment that leads to interoperability between different cloud providers and users face difficulty to switch between providers.

**Usability:** Most of authentication and authorization protocols are complex and difficult to use, which leads users to error which in turn results in security issues.

**Threat Model:** Most of authentication protocols focus on a specific threat model ignoring other existing threat models, however all existing threat models should be given equal consideration.

**Ease of use:** the authentication protocols should be easy to understand with user friendly interface and complex one may irritate users.

**Limited research on multi cloud environment:** Most authentication protocol focus on a single cloud environment, however with the increase of multi-cloud environment there is a strong need to manage keys across multiple clouds.

**Lack of focus on scalability:** Many protocols are designed by keeping focus on small cloud environment, as the cloud environment scales up it is required for authentication protocols to meet demands.

So there is need of research in above discussed fields.

III. CONCLUSION

Authentication and key management protocols are essential for providing security in cloud computing environment. This paper provides a survey of various authentication protocols provided by various researchers present in this world. This paper also demonstrate various cloud computing models and types of services provided by them. This paper also points out various research gaps in the existing systems that needs to be focused in further research.

REFERENCES


A robust IoT-based three-factor authentication scheme for cloud computing resistant to session key exposure.


