

# A Survey on Modified Pattern Based Approach for Minimizing Security Challenges in Cloud Computing

Shah Juhi Dipan<sup>1</sup>, Nirav Y. Shah<sup>2</sup>

<sup>1</sup>M.E Student, Silver oak College of Engineering & Technology, Gota, Ahmedabad, Gujarat, India

<sup>2</sup>Asst. Prof, Silver oak College of Engineering & Technology, Gota, Ahmedabad, Gujarat, India

**Abstract**—Finding the proper pattern to take care of a specific security issue is difficult on account of the nonappearance of a scientific classification scheme for security designs. An appropriate classification pattern helps efficient capacity and recovery of data, beneficial for both programming designers and software pattern analyzers. In this paper, we give a novel approach to apply and check security designs and assess different classification patterns for better security of data over cloud. Our proposed pattern utilizes security ideas to efficiently send the problem and solve it with hybrid approach of using SHA, HMAC & RSA 256 bit encryption technique in efficient way. In this paper, we are solving pattern navigation problem between client and server.

**Index Terms**—Cloud Computing, Client-Server Architecture, Encryption Techniques, Modified Pattern Based Approach, Security

## I. INTRODUCTION

In recent years, the concept of cloud computing has grown from an emerging innovative architecture to one of the fastest growing IT segments. Cloud computing is a new paradigm that combines several computing concepts and technologies of the Internet creating a platform for more agile and cost-effective business applications and IT infrastructure. Economic benefits make cloud computing systems a very attractive alternative to traditional IT systems. Cloud computing simply means Internet computing generally the internet is seen as collection of clouds; thus the word cloud computing can be defined as utilizing the internet to provide technology enabled services to the people and organizations. It is a pay as peruse kind of service, hence has become very popular in very less time. According to National Institute of Standards and Technology (NIST), "Cloud computing is a model for enabling ubiquitous, convenient, ondemand 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." Cloud computing provides more options to users because the data storage and processing are primarily handled by the cloud computing vendors. Therefore, the data is stored on a remote location, which leaves the user without an exact understanding of the storage location. The most important of these issues is the data security and how cloud providers assure it. Since cloud computing is a utility available on net, so various issues like user privacy, data theft and leakage, eaves dropping, unauthenticated access and various hackers' attacks are raised. These unsolved security issues of authentication, privacy, data protection and data verification are main hindrance for widespread adoption of cloud computing. So, for efficient data security we need a mechanism that provides secure data. So providing security by using modified pattern based approach makes the data more secure.

## II. BACKGROUND THEORY

### A. Overview of cloud computing

Cloud computing is new utility of the century, which many enterprises wants to incorporates in order to improve their way of working. It implies sharing of computing resources to handle applications. Cloud computing offers reduced capital expenditure, operational risks, complexity and maintenance, and increased scalability while providing services at different abstraction levels, namely Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). Storing or sharing data in cloud environments would make data access easier, on-demand availability possible, at much lower cost with an enhanced collaboration capability, integration and analysis cheaper on a shared platform. There are many well known service providers in the market, such as Google, Amazon, Yahoo, and Microsoft. There are also some vendors who provide cloud services in various deployment

models and service models. Cloud Computing is a term used to describe both a platform and type of application. As a platform it supplies, configures and reconfigures servers, while the servers can be physical machines or virtual machines. On the other hand, Cloud Computing describes applications that are extended to be accessible through the internet and for this purpose large data centers and powerful servers are used to host the web applications and web services. Cloud Computing differs from traditional computing paradigms as it is scalable, can be encapsulated as an abstract entity which provides different level of services to the clients, driven by economies of scale and the services are dynamically configurable.

**B. Working of Cloud Computing**

To understand the workings of a cloud computing system, it is easier to divide it into two sections: the front end and the back end. They are connected to each other through a network, usually the Internet. The front end is the side of the computer user or client. The back end is the “cloud” section of the system. The front end consists of the client’s computer or computer network and the application essential to access the cloud computing system. On the back end of a cloud system, there are various computers, servers and data storage systems that make up the “cloud”.

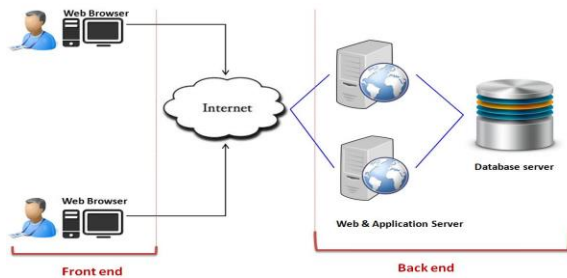


Figure-1: Working of Cloud Computing [20]

**C. Types of Service Model**

Cloud services model are usually divided in the three main types, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS).

Infrastructure-as-a-service (IaaS): The most basic category of cloud computing services. With IaaS, you rent IT infrastructure—servers and virtual machines (VMs), storage, networks, operating systems—from a cloud provider on a pay-as-you-go basis. E.g.- Amazon, GoGrid ,3Tera.

Platform as a service (PaaS): Platform-as-a-service (PaaS) refers to cloud computing services that supply an on-demand environment for developing, testing, delivering and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network and databases needed for development .E.g.- Google’s App Engine, Force.com. Software as a service (SaaS): Software-as-a-service (SaaS) is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their phone, tablet or PC. E.g. - Google, Salesforce, Microsoft.



Figure-2: Cloud Service Models [21]

**D. Types of Deployment Model**

Cloud deployment model are usually divided in the four main types, Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud.

Public cloud: Public clouds are owned and operated by a third-party cloud service provider, which deliver their computing resources like servers and storage over the Internet. Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software and other supporting infrastructure is owned and managed by the cloud provider. You access these services and manage your account using a web browser.

Private cloud: A private cloud refers to cloud computing resources used exclusively by a single business or organization. A private cloud can be physically located on the company’s on-site datacenter. Some companies also pay third-party service providers to host their private cloud. A

private cloud is one in which the services and infrastructure are maintained on a private network.

Hybrid cloud: Hybrid clouds combine public and private clouds, bound together by technology that allows data and applications to be shared between them. By allowing data and applications to move between private and public clouds, hybrid cloud gives businesses greater flexibility and more deployment options.

Community cloud: Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party, and either hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.

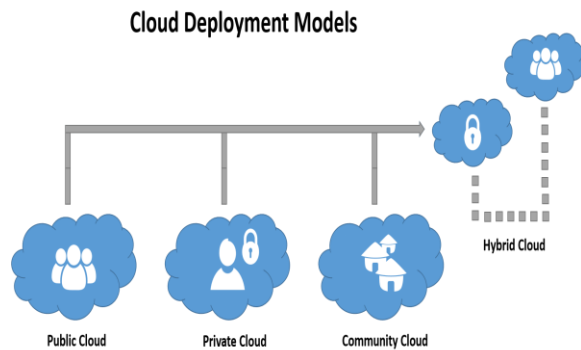


Figure-3: Cloud Deployment Models [22]

*E. Need for Security in Cloud Computing*

All the data is transferred using Internet data security is major concern in cloud computing to protect information, data applications and infrastructure associated with cloud computing. The security of data of the user is prime responsibility of cloud provider. Security is an important task as individuals and organizations have to move their private and personal important data to the cloud. Securing data remains an important priority of cloud managers to prevent global cloud security threats. So, for efficient data security we need a mechanism that provides secure data. So providing security by using modified pattern based approach makes the data more secure. The patterns which have been used till today have some strength and weakness. So we need some patterns that will help in secured data.

*F. Security Challenges In Cloud Computing*



Figure 4: Security is the Major Issue [23]

Some security challenges are listed and discussed below:

Data Loss: Data loss is any process or event that results in data being corrupted, deleted and/or made unreadable by a user and/or software or application. It occurs when one or more data elements can no longer be utilized by the data owner or requesting application. Data loss is also known as data leakage.

Intrusion: In intrusion someone or something is trying to compromise information system through malicious activities or through security policy violations.

Insecure application: Application vulnerability is a system flaw or weakness in an application that could be exploited to compromise the security of the application.

Theft of credentials: Credential theft occurs when an unauthorized person (attacker) obtains and uses valid account credentials (username and password) for unauthorized access to a computer.

Anytime stop (Denial-of-service): A denial-of-service attack is a security event that occurs when an attacker takes action that prevents legitimate users from accessing targeted computer systems, devices or other network resources.

Less Reliable for data process and storage: Less trusted for data process and storage as both data process and storage are done through net.

Improper (malicious) use of services: Malware, or malicious software, is any program or file that is harmful to a computer user. Malware includes computer viruses, worms, Trojan horses and spyware. These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission.

### III. RELATED WORK

Schumacher et al. <sup>[14]</sup> propose patterns specifically for security. The authors defined simple solutions to security problems during the software engineering design and implementation phases. The resulting pattern catalogues support specifically design and implementation phases of software engineering processes, while our work focuses on the analysis phase of software engineering.

Hafiz <sup>[15]</sup> described four privacy design patterns for the network level of software systems. These patterns solely focus on anonymity and unlink ability of senders and receivers of network messages from protocols, e.g., HTTP. The works of Fernandez et al. and Hafiz focuses exclusively on specific kinds of systems: Voice-over-IP and network-based software systems. We focus on any kind of cloud computing system.

Security challenges based on cloud types: Kuyoro et al <sup>[16]</sup> studied the cloud computing security issues and challenges by focusing on the cloud deployment and service delivery types. Clouds can be deployed as three different models, Private, Public or Hybrid clouds <sup>[16]</sup>. Authors stated that the private clouds are much safer than public clouds since all cloud resources are managed by the organization that maintains the cloud. Public clouds, typically a pay-per-use model poses a security threat, since the data is shared with an off-site third-party provider. Hybrid cloud is a combination of private and public clouds that provide more control over the data, and also various users can access those data through the Internet. In this classification model <sup>[16]</sup>, authors failed to compare the cost models in maintaining these deployment models and security trade-offs.

Security challenges based on cloud deployment models: Ramgovind et al. <sup>[17]</sup> explained three broad deployment models: Infrastructure as a service (IaaS), Software as a service (SaaS) and Platform as a service (PaaS) and highlighted security issues that are specific to each deployment model. Upon deciding on a cloud delivery model (Private, Public or Hybrid) and deployment model (IaaS, SaaS or PaaS), authors enumerated the security concerns that security professionals and users should be aware of in the current cloud computing environment. The authors incorporated several security issues emphasized by Gartner <sup>[18]</sup> into their investigations on information security issues when dealing with cloud computing,

which are privileged access, regulatory compliance (external audits, security certifications, etc.), data location (client's control over the location), data segregation (is encryption available at all stages to all clients?), recovery (disaster management), investigative support (ability to investigate illegal/inappropriate activities), long term viability (if a vendor goes out of business), and data availability (if the vendor moves to a different environment).

Fernandez et al. <sup>[19]</sup> design several UML models of some aspects of Voice-over-IP (VoIP) infrastructure, including architectures and basic use cases. The authors also present security patterns that describe countermeasures to VoIP attacks. Our work provides additionally tool support and requirements validation. We can also envision to use the models and information from Fernandez et al. to provide an adaptation of our approach for VoIP scenarios.

### IV. CONCLUSION

All the data is transferred using Internet data security is major concern in cloud computing to protect information, data applications and infrastructure associated with cloud computing. The security of data of the user is prime responsibility of cloud provider. Security is an important task as individuals and organizations have to move their private and personal important data to the cloud. Securing data remains an important priority of cloud managers to prevent global cloud security threats. So providing security by using modified pattern based approach makes the data more secure. Since there is no specific process to support evolution or classification of security patterns, subject descriptor pattern ,secure proxy pattern, authentication and authorization, web agent interceptor pattern ,credential synchronized pattern can be verified and tested. A novel approach is needed to apply for better security designs and assess different classification patterns for better security of data over cloud. Our proposed pattern utilizes security ideas to efficiently solve the problem which can be a hybrid pattern that applies multiple key encryption.

### REFERENCES

- [1] Priya Anand, Jungwoo Ryoo and Hyounghick Kim, "Addressing security challenges in cloud computing –a pattern-based approach", 978-1-5090-1078-3/16 \$31.00 © 2016 IEEE DOI 10.1109/ICSSA.2015.11

- [2] Battista Biggio, Giorgio Fumera, Fabio Roli, "Security evaluation of pattern classifiers under attack", IEEE, 2014
- [3] Bin Feng, Xinzhu Ma, Cheng Guo, Hui Shi, Zhangjie Fu, Tie Qiu, "An Efficient Protocol with Bidirectional Verification for Storage Security in Cloud Computing", 2169-3536 (c) 2016 IEEE DOI 10.1109/ACCESS.2016.2621005, IEEE Access
- [4] Nobukazu Yoshioka, Hironori Washizaki, Katsuhisa Maruyama, "A survey on security patterns", ©2008 National Institute of Informatics DOI:10.2201/NiiPi.2008.5.5
- [5] Jin He, Kaoru Ota, Mianxiong Dong, Laurence T. Yang, Minyu Fan, Guangwei Wang, and Stephen S. Yau, "Customized Network Security for Cloud Service", 1939-1374 (c) 2017 IEEE DOI 10.1109/TSC.2017.2725828, IEEE
- [6] Mrs. Rupali Sharma and Dr. Bharti Joshi, "H-IBE: Hybrid-Identity based Encryption Approach for Cloud Security with Outsourced Revocation", 978-1-5090-4620-1/16/\$31.00 ©2016 IEEE
- [7] Joonsang Baek, Quang Hieu Vu, Joseph K. Liu, Xinyi Huang, Yang Xiang, "A secure cloud computing based framework for big data information management of smart grid+", 2168-7161 (c) 2013 IEEE DOI 10.1109/TCC.2014.2359460, IEEE
- [8] Kristian Beckers, Maritta Heisel, Isabelle Côté, Ludger Goeke, Selim Güler, "Structured Pattern-Based Security Requirements Elicitation for Clouds", IEEE, 2013
- [9] Hanane Bennasar\*, Mohammad Essaaidi, Ahmed Bendahmane, Jalel Ben-othman, "State-of-The-Art of Cloud Computing Cyber-Security", IEEE, 2015
- [10] Virendra Singh Kushwah\*, Aradhana Saxena\*\*, "A Security approach for Data Migration in Cloud", International Journal of Scientific and Research Publications, 2013
- [11] Mr. Prashant Rewagad, Ms. Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", IEEE, 2013
- [12] Neha Tirthani, Ganesan R., "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography", IEEE, 2013
- [13] <https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/>
- [14] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann, and P. Sommerlad, "Security Patterns: Integrating Security and Systems Engineering. Wiley, 2006.
- [15] M. Hafiz, "A collection of privacy design patterns," in PLoP, ser. PLoP '06. ACM, 2006, pp. 7:1–7:13.
- [16] SO, Kuyoro. "Cloud computing security issues and challenges." International Journal of Computer Networks, 2011.
- [17] Ramgovind, S., Mariki M. Eloff, and E. Smith. "The management of security in cloud computing." Information Security for South Africa (ISSA), 2010. IEEE, 2010.
- [18] Brodtkin, Jon. "Gartner: Seven cloud-computing security risks", 2008.
- [19] E. B. Fernandez, J. C. Pelaez, and M. M. Larrondo-Petrie, "Security patterns for voice over ip networks," in ICCGI. Washington, DC, USA: IEEE Computer Society, 2007, pp. 19–29.
- [20] <https://www.guru99.com/cloud-computing-for-beginners.html>
- [21] [https://en.wikipedia.org/wiki/cloud\\_computing](https://en.wikipedia.org/wiki/cloud_computing)
- [22] <https://www.uniprint.net/en/7-types-cloud-computing-structures/>
- [23] <http://www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt> at slide 17