A STUDY PAPER ON DATA SECURITY TECHNIQUES IN CLOUD COMPUTING

Priyanka Paygude[1], Vishwas Katiyar[2], Jaya Kumari[3], Sanchita Shrivastava[4],Manisha Kasar[5]
[1]*Associate Professor, Bharati Vidyapeeth (Deemed to be University), College of Engineering, Pune*
[2]*Student, Bharati Vidyapeeth (Deemed to be University), College of Engineering, Pune*
[3]*Student, Bharati Vidyapeeth (Deemed to be University), College of Engineering, Pune*
[4]*Student, Bharati Vidyapeeth (Deemed to be University), College of Engineering, Pune*
[5]*Assistant Professor, Bharati Vidyapeeth (Deemed to be University), College of Engineering, Pune*

Abstract- Cloud Computing has become one of the fastest emerging technology in recent times in the field of computer science. As the new pattern of service in computing, is developing rapidly and its security issues have become a major part of the topic of discussion. The sensitive data (health, finance, personal information, etc.) have a very important value, and any infringement of privacy can cause great loss in terms of money and reputation for the organization as well as the individuals. So that is the confidentiality of the data is the major part of cloud computing. In this paper, we provide a survey on privacy risks and challenges for public cloud computing and therefore also present and analyze the main existing solutions that have made great progress in this area.

Keywords *- Privacy, cloud computing, data confidentiality, privacy techniques, Trusted Platform Module, Trusted Third Party Mediator, Sticky policy, Encryption, Obfuscation.*

I. INTRODUCTION

Cloud computing is defined by the United States National Institute of Standards and Technologies (NIST) as "Cloud Computing is the model for delivering the computing services which includes servers, storage, databases, networking, software, analytics, moreover the Cloud (Internet)" [1]. The same NIST document describes five main cloud characteristics (on-demand self-service, broad network access, multi-tenancy, rapid elasticity, and measured service), its three service models (SaaS: Software as a Service, PaaS: Platform as a Service, IaaS: Infrastructure as a Service) and some cloud deployment models (public, private, hybrid and community)[2].

Cloud Computing provides an alternative to premises datacentre. They also provide a wide variety of software and platform as a service. Now coming to the security of this platform, in general, privacy issues are not recent matters. Around the world, this has driven the release of a large number of laws and legislation to ensure the protection of individual data. Examples include the Fair Information Practices [3], the European Directive [4], the USA Health Insurance Portability and Accountability Act (HIPAA)[5], A. Ghorbel, et al, the USA Gramm–Leach–Bliley Act [6] etc. Privacy issues become more and more hazardous in the cloud computing environment. So, these laws may not be applicable in such a dynamic and public environment and they need to be customized to cover all privacy problems.

II. DATA PRIVACY TECHNIQUES

A.Trusted Platform Module

It is one way to establish trust between the provider of the cloud computing infrastructure and his customers in cloud computing. The Trusted Computing Group has defined the most widely used method of Trusted Computing technology (TCG). The TCG suggests that trustworthy software and hardware components be added to standard computer platforms [7]. Trusted Computing allows for the creation of trusted execution environments in basic cloud infrastructures. Concerning the common assumption; it is said that software cannot be completely secured when it is alone. It has to be assisted with the hardware [8]. This is why Trusted Computing Group has specified the internal architecture of the trusted platform module is represented here [9]. It suggests that the TPM is the only device which can be used as tamper-resistant and also be used in the open physical platform for the pc.

The paper by Mr Kailash Patidar et al [11] represents a new paradigm in cloud computing information protection and security. They investigated and defined a novel cloud computing trust model, as well as addressed the basic security concern of utility cloud computing with multi-tenancy. This method benefits both operators and clients.

The situation where TPM can be applied is where we want to provide an extra layer of security for operations, storage, communications, monitoring, and so on. The limitation which we analyzed in this technique is that it does not take initiative to perform any action on its own. There is no way to tamper-resistant on it. It responds to the only particular commands.

B.Trusted third-party mediator (TTPM)

A trusted third party will act as a mediator (TTPM) between the client and the cloud component to ensure policy

compliance and to conduct research. This process is not new; it was adopted to build online customer trust when using e-commerce applications. For example, a reputable third-party company may act as an anonymous client who hides information that identifies a customer. In addition, TTPM was used to maintain. QoS (Quality of Services) on a specific QoE-based (Quality of Motivation) platform. It is also used to test the cloud component whether complies with customer preferences when managing private data in the cloud and conducting research and control. Ideally, a reliable external company should evaluate each request for data processing that may have a significant impact on system performance.

By reviewing the paper of Susmita **J A Nair et al [12]** we came to know that Cloud computing is an emerging platform in the distributed computer sector that provides web-based, accounting, and storage services community (including business, health, and government). Customers are provided with flexible services and thus cloud users benefit economically on a large scale. However, security is a major concern for cloud users. Some of the areas of concern for cloud computing security are database, data transfer time, user authentication, etc. In the cloud space, anyone can access data via the internet. Therefore user authentication and access control are very important in the cloud. Trusted third parties are independent service providers and are considered to have some degree of trust. A trusted foreign company facilitates secure communication between the two companies that trust this foreign company. Cloud service providers have user data control and accounting services. A trusted external company guarantees the integrity of the database.

C. Sticky policy

Sticky policies, conditions, and limitations ensure how the data should be treated, and connected directly to the corresponding data. Sticky policies can control how data can be accessed and used throughout their life cycle, to allow access control decisions and implementation of the policy which must be done in a distributed manner. In this way, a smart control in the protection of sensitive information, about individuals and businesses, is achieved. Such a method was introduced primarily for data enforcement privacy and other rules, when you send information to a data buyer, the user/producer/owner agrees to the active policies that select the preferences you wish.

The paper by Sabrina Sicari et al[13], IEEE member, introduced a paradigm of policy that Sticky policy is one of the emerging ways to improve security as well privacy features on online-based systems. In the digital age, where the Internet connects things around the world and people live online, data security and privacy become the key drivers (and barriers) of change to embrace new solutions. In traditional methods, their communication links are encrypted, and access control is statically controlled by the central office, indicating their limitations when used on large, connected, and distributed systems. The regulations, while distinct, still exist to adapt to technological and social changes, and to protect confidential information about governments, businesses, and individual citizens. In this case, appropriate methods should be defined to allow for strict control over the data life cycle as well we guarantee the privacy and enforcement of certain laws in the disclosure of personal information, use, and access. Sticky policies represent one way to improve owners' control over their data. In such a way, the machine-readable policies are the same attached to the data. They are called 'attachments' because they go hand in hand with data, as the data travels across multiple administrative domains.

This paper explores the state of the art in Sticky policies, and discusses limitations, open issues, applications, and research challenges, with a special focus on their use of the Internet of Things, cloud computing, and Content-Centric Networking. The study of state of the art regarding the actual application of sticky policies to promote privacy in the context of data sharing among different data users was analyzed. Many open challenges have been highlighted, thus providing some light on industry research and guidelines in this field.

Dealing with such problems will allow for a Sticky policy that modifies and ensure high levels of security and privacy in various application domains and IT industries.

The paper by Jakub Sendor et al[14] introduces one of the major security concerns related to cloud hosting and virtualization, which is the lack of reliance on infrastructure. This lack of trust is due to the lack of transparency regarding data management and storage conditions. No valid technical guarantees are available to convince a potential cloud customer to take full advantage of his or her data. In this paper, we recommend a security service (called SPACE) in the cloud that gives all the tools to the data owner to force his privacy preferences during the action phase. SPACE is based on Sticky policy technology and provides access to and implementation control performance data anywhere in the cloud. In addition to the key security features offered by SPACE, new one’s imagination and control are proposed to do the user fully aware of his or her privacy status information.

In this paper**, Jakub Sendor et al[15]** proposed a Privacy Policy engine used as a cloud service that ensures access to and controls the use of data. The development of such a solution was inspired by the lack of transparency and control of perceived data in various forms of commercial cloud infrastructure

This service, SPACE, provides an opportunity for the data owner to permanently control again his data in the clouds throughout his life. SPACE is based on the application of Sticky policies attached to data and possible enforcement of

privacy laws anywhere in the infrastructure. The goal of this solution is to maintain the confidentiality of data stored in the cloud to protect it from unauthorized access, by forcing obligations related to their use and full provision control and visibility to the user to be the only master of his data. A few enhancements and extensions are available right now under investigation, especially regarding your concerns about performance improvements and local performance data in cloud infrastructure (where data is stored, repeated and processed). Audit and service certificates are important factors that we plan to address in turn to provide the most reliable guarantees on the solution.

D..Encryption

Encryption is the process of converting data from its original plaintext format to an unreadable format, such as a ciphertext, before sending it to the cloud for storage.
Encryption uses sophisticated algorithms to scramble data, which makes no sense to users without keys. Authorized users use the key to decrypt the data and convert the hidden information back into a readable format. A key is generated and shared only with trusted parties. The identification of a trusted party is established and verified by some form of multi-factor authentication.

Faraz Fatemi Moghaddam et al [16] present a model based on separate data and key cloud servers and a client-based data encryption service for increasing the reliability in cloud computing environments in their survey paper. The key generation process is done in a separate cloud application in the proposed paradigm, and public and private keys are stored in key cloud servers. These techniques were briefly presented and then recreated in the same situation for the simulation process to assess the performance of client-based data encryption services. According to the findings, E-RSA is the best acceptable algorithm for use in client-based data encryption services since it achieves acceleration, accuracy, and security in this service based on compatibility issues.

On Further discussion, we reviewed a paper *by* Rachna Arora et al [17].In this paper, they have discussed cloud computing security issues, mechanisms, and challenges that cloud service providers face during cloud engineering and presented the metaphoric study of various security algorithms. This article proposes cryptographic algorithms to make cloud data secure and vulnerable, creates security issues and challenges, and compares AES, DES, Blowfish, and RSA algorithms to cloud data in cloud computing. I have found the best security algorithm that I need to use to be secure. . By implementing all the algorithms in the IDE tools and JDK 1.7, the output required for cloud computing data was achieved. With the growing demand for the cloud in today's world, cloud and user security are top priorities. Therefore, the proposed algorithm will serve today's needs. In the future, some comparisons with different approaches and results may be provided to demonstrate the effectiveness of the proposed framework.

E. Obfuscation

Data obfuscation is a process to obscure the meaning of data as an added layer of data protection. In the event of a data breach, sensitive data will be useless to attackers. The organization and any individuals in the data will remain uncompromised. Organizations should prioritize obfuscating sensitive information in their data.
The most obvious and essential benefit of data obfuscation is hiding sensitive data from those who are not authorized to see it. There are benefits beyond simple data protection.

This paper by Khaled M. Khan [18], proposes an approach to data obfuscation when matrix multiplication is offloaded to cloud computing. It is primarily based on splitting the rows and columns of a matrix to change the actual dimensions, adding and mixing random noise to ensure confidentiality and privacy. In this approach, obfuscated matrices are sent to the server without public-key encryption. While computing on a matrix, the server cannot extract or derive the actual value from the obfuscated matrix or the calculated multiplication result. The client, on the other hand, can extract the actual complexity from the server-generated results with a small amount of computation.

In this approach, the client is required to spend an insignificant effort to split the matrices. It would not Cost more than O(n). The client can compute the process of splitting their matrices using handheld low-powered devices. This technique does not need any encryption, so that, the cloud server does not need decryption of the matrices. The cloud server does only matrix multiplications and does not require any additional computation due to splitting of matrices, introducing noise to values, and shuffling of rows. Used in this context Data obfuscation technology in computing is outsourcing field of cloud computing.

Strengths and Weakness of the techniques.

Techniques	***Strength***	***Weakness***	***Application***
Trusted Platform Module	Provides the location which is shielded to protect the user's confidential data. Provides flexible security services for the users.	Cannot perform secure processing. Only presents a hardware solution.	Used for system integrity measurements and for key creation and use.
Trusted Third Party Mediator	Allows a third party to verify that the privacy policies are being followed.	High level computation is added because of the additional communication traffics.	Facilitates secure communication between two parties who trust this third party.
Sticky Policy	Binds data to policy, allowing processing only when the policy is followed.	Contributes a large amount of cost.	Used to generate a symmetric key under IBE(Identity-based Encryption) for AES(Advanced Encryption standard).
Encryption	Enables strong data protection when data is at rest but also supports any type of data.	Makes the indexing and searching difficult.	Used to protect data in transit and data at rest. Encryption is used to protect the information being relayed.
Obfuscation	Permits concealed data to be calculated with appropriate accuracy.	Weak protection than encryption.	Used to hide the behavior of the source code of complex algorithms to hide implementation details. Used to protect intellectual property .

III. CONCLUSION

In this paper,we had surveyed and enlisted several techniques that can be followed to solve the issues of data secur y in cloud computing.Now, these approaches u s some techniques which can lead to,,the solution for user data security problems in cloud computing and thus, confidentiality of the data can be maintained by using the these techniques.Though more techniques are yet to come and can be later added with these techniques to enhance the security in this field.The reasearchers could take this paper as a reference to deal with data privacy issues .

IV. REFERENCES

[1] Mell P, Grance T (2011) The NIST definition of cloud computing .

[2]. S. Berger, R. C´aceres, K. A. Goldman, R. Perez, R. Sailer, and L. van Doorn. vTPM: virtualizing the trusted platform module. In Proc. of USENIX-SS'06, Berkeley, CA, USA, 2006.

[3] US Privacy Protection Study Commission (1977) Personal Privacy in an Information Society-the Report of the Privacy Protection Study Commission.

[4] Directive EU (1995) 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Off J EC 23.

[5] Act HIPAA (1996) Health insurance portability and accountability act of 1996. Public Law 104:191 123 A. Ghorbel et al.

[6] Code US (1999) Gramm-Leach-Bliley Act. Gramm-Leach-Bliley Act/AHIMA, American Health Information Management Association.

[7] "Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1b", Published by the Trusted Computing Group, 2003.

[8] Jason Reid Juan M. González Nieto Ed Dawson, "Privacy and Trusted Computing", Proceedings of the 14th International Workshop on Database and Expert Systems Applications, IEEE, 2003.

[9] Mohammed Achemlal, Sa¨ıd Gharout and Chrystel Gaber Orange Labs - France Telecom.

[10] Zhidong Shen, Li Li International School of Software State Key Laboratory of Software Engineering.

[11] Mr. Kailash Patidar ,Mr. Ravindra Gupta,Prof. Gajendra Singh ,Ms.Megha Jain,Ms.Priyanka Shrivastava.

[12] S., Castell. Code of Practice and Management Guidelines for Trusted Third Party Services. s.l.: INFOSEC Project Report S2101/02, 1993

[13] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, "Security towards the edge: Sticky policy enforcement for networked smart objects,"

[14] G. Spyra, W. J. Buchanan, and E. Ekonomou, "Blockchain and git repositories for sticky policies protected ooxml." Vancouver, Canada, 2017.

[15] Jakub Sendor, "On using encryption techniques to enhance sticky policies enforcement," 2008.

[16] Faraz Fatemi Moghaddam, Omidreza Karimi, and Maen T. Alrashdan , A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments.

[17] paper Rachna Arora, Anshu Parashar / International Journal of Engineering Research and Applications (IJERA).

[18] Khaled M. Khan, Faculty of KINDI Computing Lab, Qatar University.