International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Cloud Secured: A Study on Cloud Computing Security

Sukhvinder Singh Bamber *[1]

Submitted: 16/11/2022 **Revised**: 18/01/2023 **Accepted**: 17/02/2023

Abstract*:* A method of service delivery is cloud computing. Over the network, computing resources are made available as a service. These services have the characteristics of being Scalable, Autonomous, and Economical. A new approach is required to help end users and providers of services better understand the domain so they can handle their security needs and find their solutions. Despite having so many benefits, it faces a number of security issues that cannot be disregarded. There are various precautions that must be taken against the risks posed by the cloud computing model in order to increase cloud computing's security and dependability. Cloud security is one of the main concerns on interested parties' minds. While evaluating the security challenges in cloud computing, each concern has a variety of repercussions on specific assets. Despite numerous research, we are still unable to specify the security requirements, which slows down the use of clouds. A new technique is consequently required to assist service providers and target users in better understanding the domain, managing their security requirements, and finding solutions. The "ontology-based security approach" is one of many security measures employed by related stakeholders. However, target users and cloud service providers find it complicated and deficient in the security department because it is not specified which paradigm can be utilised under which circumstances. Prior studies have revealed a number of security concepts that service providers with various assessment methods can utilise. Consequently, there is a growing demand for a critical evaluation of earlier research on Cloud Security Ontology. Further, in order to assist researchers in linked fields, future prospects for research based on comparison analysis and deficiencies areas have been looked into. Associated cloud computing risks are outlined in this study, along with any potential remedies.

Keywords: *Cloud Computing, Cloud Security, Cloud Infrastructure, Encryption, Security Key.*

1. Introduction

Cloud Computing is the availability of any computer service on demand by paying for it such as online applications, remote computing resources, storage, databases etc. via Internet or network. With respect to the rising demand for cloud computing services, the demand for cloud computing expertise is also rising at the moment. It offers three major types of service models Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In order to detect, analyse, and elicit security countermeasures, it conducts a systematic review and creates a conceptual link among entities that represent information [1]. Due to the fact that small and large businesses alike have begun using cloud services, as such have a choice of deploying different types of clouds: private, public, community or hybrid clouds, depending on their requirements [2].

The use of cloud computing services has expanded from small to large organisations, putting it one of the most demanding technologies of the time. Where several cloud deployment alternatives are employed and cloud services are offered in accordance to the requirements, internal and external security is maintained to keep the cloud system protected. There is a significant issue with safeguarding cloud infrastructure, data and applications against unauthorised users, DDOS attacks, viruses, hackers, and other related threats. This is known as cloud computing security.

Depending on the deployment method and service objectives, there are 4 types of clouds: private, community, public and hybrid clouds.

Four main types of cloud computing:

1.1 Private Cloud

Cloud services typically operate on a single-tenant (exclusive) basis environments that come with all the features and advantages of freedom and the responsibility model of cloud computing. They are provided by corporations or their chosen service providers [3]. Private cloud storage options, like COSA (Cloud Object Storage Appliance) and Oxygen Cloud, offer businesses file synchronisation and sharing with high performance and built-in security [4].

1.2 Public Cloud

An operational platform that is either solitary (dedicated) or multi-tenant (mixed), with all the advantages and capabilities of the mobility and responsibility of the cloud

[1] *Computer Science & Engineering, University Institute of Engineering & Technology, Punjab University SSG Regional Centre, Hoshiarpur, Punjab, India.*
ORCID ID : 0000-0002-1749-2940
** Corresponding Author Email: ss.bamber@pu.ac.in*

model, is provided by public clouds, which are delivered by a specific CSP. Software and data core infrastructure form a public cloud that is managed by outside organizations, such as Google and Amazon, and that makes its services available to businesses and customers online [5]. Variations among public and private clouds can be found [6] by contrasting the characteristics of two kinds of clouds as listed in Table 1.

1.3 Community Cloud

Community Clouds are made available by a reputable service provider affiliated with a particular community and offer either a single (limited) or multi-tenant (shared) workflow with all the advantages and potential of flexibility and the cloud model's accountability.

1.4 Hybrid Cloud

Irrespective of ownership or location, hybrid clouds mix public and private cloud designed to help unidirectional information sharing as well as potential application scalability and mobility across different Cloud service offers and providers [7]. NIST (National Institute of Standards and Technology) describes a hybrid cloud environment as a "composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability" [8].

Service delivery model of the cloud are (Fig. 1.):

1.4.1 SaaS - Software as a Service

SaaS differs greatly from traditional software in both its technical architecture and its commercial architecture [9]. The ability to utilise the company's apps running on cloud computing and reachable from a number of client devices utilising a light network connection like a Web browser is the functionality made available to the consumer (e.g., web-based email). SaaS platforms make it easier to construct applications by giving users access to development tools, abstraction layers, and software components that are ready to use [10].

1.4.2 PaaS - Platform as a Service

The user can utilise the computer tools and languages supplied by the provider to deploy consumer-created apps on the cloud computing (example - java, .Net, python). Platform as a Service concentrates on giving developers access to Language Runtime and Services while leaving the provisioning and management of Infrastructure to the underlying Layer [11].

1.4.3 IaaS - Infrastructure as a Service

The end users have the flexibility and choice of leasing remote computing power, storage and various other computer resources. Eucalyptus [12], Nimbus/Cumulus [13], Open Nebula [14] and Open Stack [15] are the main rivals in the open source IaaS cloud branch. The user can deploy and run any computing resources where the consumer, including applications and operating systems, using these resources [16].

Table 1. Difference between Public and Private Cloud

Item	*Public Cloud*	*Private Cloud*
Pattern of service	SaaS, PaaS, IaaS	SaaS, PaaS, IaaS
Object of service	Internal organization of enterprise or community	General Public
Ownership of infrastructure	Enterprises	Cloud service providers
Mode of deployment	Enterprises	Cloud service providers
Quality of service	Individual service with more stable network	Not individual enough service and unstable network
Privacy of data and security	Reliable enterprise interior and controllable data	CSP may peep into existing information
Influence on existing IT management process	Hardly effect	Enormous implications

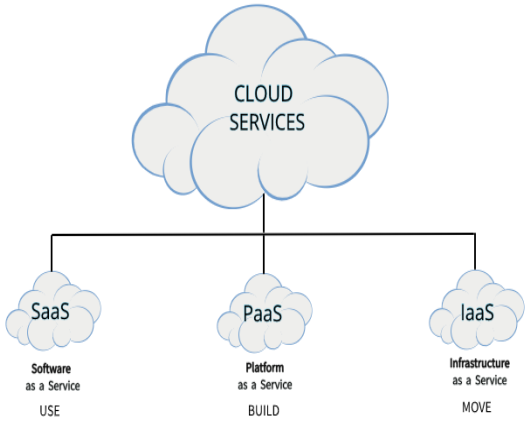

Fig. 1. Cloud Services

1.5 Features of the Cloud Computing

According to relevant domestic and international research benefits that can be summed up in three categories [17]:

- Cloud Server Terminal - The component of providing, overseeing, and maintaining a service on the cloud server. It consists of large number of PCs and servers that are fast, efficient, highly reliable, and cost-effective [18].
- Middle connection terminal - The network device that connects the cloud server and the client terminal and lessens their reliance on one another is called the middle connection terminal. It possesses characteristics like looseness, coupling, extensive coordination, real-time synchronisation, etc.
- User terminal - The client terminal is a component of renting, acquiring, and utilising cloud services. It alludes to the widely utilised terminal equipment that is versatile, affordable, shared, and environmentally friendly.

2. Literature Survey & Background

A survey of the different security threats that the cloud encounters is provided by Subashini and Kavitha [19]. The security concerns brought on by cloud service delivery paradigms are the focus of this study. Earlier research [20 - 21] has made an effort to identify cloud security concerns. A risk model for the cloud has also been created by Kamongi et al. [22], however it is not connected to any current compliance standards. The work by Popovi et al. [23] on cloud security standards and controls has mostly focussed on the cloud engineering and provider end. It is yet unclear how many cloud providers are implementing the security standards in [24 - 25] and are prepared to handle threats, which could be concerning to customers who must choose between these providers.

The cloud provider is the administrator / controller of security and privacy regulations according to NIST's cloud technology reference architecture [24 - 26]. But on the other hand, its reference architecture's security compliance model is relevant to all of the roles. For any and all cloud delivery types, the same security policies are utilised to safeguard cloud environments. The application of compliance standards to these security controls. The network, IT infrastructure, and electronic data processing are the main topics of the information technology compliance model [27]. To ensure that all of the IT components function together smoothly, compliance models apply rules and regulations to each one. On the basis of these compliance models, organisations frequently establish security controls. Gordin et al. [28] discussed the possibilities of an open cloud in 2018. In contrast to open clouds, where vendors have maintained security, experts have suggested that private clouds are more concerned with security. This Openstack Pike version's security was examined and explained by the author. Both externally and internally, security is examined. The researcher also examines and discusses containment of hypervisor-based virtual servers in the study. Therefore, a conclusion is deduced from the multi-tenant setting. Lattice computation and distributed computing were the perspectives Jujare [29] used to explore computer technology. According to the client's fundamentals as well as the pay for use front, this provides enormous IT organisations to the end user here on system. The researcher Kumar focussed on the security of cloud computing in hid research work on security threats utilizing transmission of data from one place to another. Encryption and decryption techniques are the basis of security implementation in cloud computing [30].

Bashir with Haider [31] carried out the detailed literature survey to expose the cloud computing vulnerabilities that are areas of high risk. This literature survey has also taken into account the main security risks posed by suppliers and consumers in relation to cloud hosting by analysing various security mechanisms and solutions. The Cloud Security Alliance developed a Trusted Cloud Initiative Reference Architecture [32]. The design suggested in the literature aims to give a straightforward yet precise cloud infrastructure by outlining the potential roles of the entities inside this cloud computing system as well as their system accessories and operations.

2.1 Background

The Background section gives some details about the architecture of cloud computing systems and talks about topics such as preliminary data security [33]. The actor-based approach employed by NIST is also used in the suggested cloud computing architecture [34]

2.1.1 Security Service

Security encompasses all methods intended to safeguard, fix, and ensure that data in computer systems is protected from a variety of dangers. Practically, security mechanisms implement security policies via security services provided. Features like non-repudiation, confidentiality, integrity, authentication, and availability are used by computer critical infrastructure to ensure security [35]

• Information is kept private and protected against disclosure to unauthorised people, organisations, or systems. In reality, throughout transmission, no unauthorised parties should be able to view the data being sent (or received). Confidentiality can be achieved through

data encryption which can further implement symmetric / asymmetric key paradigm to establish confidentiality.

• Integrity is the mechanism of guaranteeing that the data is received by an authorised person and exactly the same as the data transmitted, with no alterations. It guarantees the data hasn't been changed by a third party, by way of explanation (either intentionally or accidentally). The connection is severed and also the spread of the bogus information is halted whenever an intrusion is detected.

• Availability is the mechanism of ensuring that the required resources and the data are available as and when requested by the authorized user, thus guaranteeing the accessibility of service to authenticated user. For instance, a source system will not be able to transfer the data successfully to the destination system if the Distributed Denial of Service (DDoS) attack takes place.

• Authentication is the process of verifying and authenticating the source as well as destination. If the identities of sender / receiver are confirmed.

• Senders and receivers cannot retract their activities thanks to non-repudiation. Repudiations come in two varieties: source repudiations and destination repudiations. Neither the sender nor the recipient may contest the message's transmission in the first case, and they also cannot contest its delivery in the second.

2.2 System Description

To better appreciate security concerns, we first must comprehend the cloud architecture which is the subject of the subsequent paragraphs. A cloud business is composed of resources that are devoted to demands.

- According to NITS, there are five main actors in cloud computing configuration.

2.2.1 Cloud End User

A cloud end-user or say cloud consumer is a person or a business organisation that makes use of cloud services. In fact, by carefully examining the products and solutions made available by cloud suppliers and entering into a deal, a cloud user can select the best services [36]. An agreement between the cloud consumer and a cloud provider (Service - Level Agreement - SLA) must be signed in order to complete this contract and specify the technical performance. Security, efficiency breakdown avoidance, and uniformity of quality of service are all covered by Service level agreement. However, a cloud customer has the option to select providers with better services and lower costs.

2.2.2 Cloud Supplier

The cloud supplier is any organisation that offers services to a cloud end user. After the installation and administration of cloud infrastructure, the cloud provider organises and arranges cloud software. According to the few cloud-based administrative tools available, for the maintenance and monitoring of infrastructure and applications, SaaS providers are primarily responsible. While for the platform's computing infrastructure management PaaS is used by the cloud provider, and cloud software is used to provide the platform's individual components (For instance, runtime applications, databases or additional middleware elements) [37]. The cloud consumers receive and make use of cloud services. Cloud privacy and security must be properly constructed since, without them, this revolutionary computing paradigm could suffer a catastrophic failure [38].

2.2.3 Cloud Auditor

A cloud auditor is in charge of carrying out evaluation, assessment, and scrutiny of cloud services' efficiency, safety, and confidentiality. Inspection ensures that cloud services meet standards and to improve their quality [39].

2.2.4 Cloud Agent

Since coordinating the implementation becomes hard for them to handle, cloud users access the cloud services through a cloud agent instead of contacting the cloud supplier directly. In actuality, a cloud agent manages transactions amongst cloud providers and clients as well as cloud delivery of services, efficiency, and consumption.

2.2.5 Cloud Carrier

Cloud carrier acts as an intermediate platform between cloud providers and customers for providing cloud services. Using the underlying network hardware, services and other access devices, cloud carriers can reach out to the customers. As was previously mentioned, cloud hosting can supply cloud users with services that adhere to SLAs by setting up the cloud SLA with a cloud carrier. Additionally, Secure connections between the cloud providers and clients are the responsibility of the cloud carrier.

2.2.6 Governance

Governance involves the choices made when it comes to the rules, procedures, and specifications that apply to all of the tasks carried out in cloud computing environments [40]. By developing regulations that address business and IT (technical) challenges from organisational relationships to related activities and processes, governance is best and most effective. Cloud services are connected to governance in cloud computing. They need to be properly handled, regulated, and sustained to improve quality and performance; as a result, techniques, processes, and technology are needed [41]. Guidelines on providing a service and who should carry out specific tasks and procedures are referred to as policies in governance. These actions can be taken to successfully manage and implement cloud computing [33].

3. Cloud Security Issues

The volume of data stored on a cloud-based system makes it more vulnerable to assaults because it might contain confidential information that could place many individuals in an unpleasant position if released [42]. It is the responsibility of data security in cloud computing to prevent the revelation of information to cybercriminals. Static and dynamic anti-virus technology are the two main types used in private cloud big data [43]. Cloud Computing provides the alternate to the organisations for a quick, adaptable, and affordable substitute for hosting their own computing resources [44]. But the security experts, hackers, and attackers have proved that this approach can be subverted and is not completely safe [45]. When data is moved, there is the greatest risk. Furthermore, since so many people have access to the server, it is easier for fraudsters to obstruct the process. Issues with data security and privacy in cloud computing include:

3.1 Data Breach

Data spill or data leakage are two terms used to describe the intentional or unintended release of sensitive data from the cloud to unauthorised individuals. In plain English, a "data breach" is when someone gains access to data they are not supposed to have. When there has been a data breach, regardless of whether it was accidental, the most often targeted kinds of data are Personal Health Information (PHI), Individually Identifiable Data (IID), Trade Secrets, and Copyright Law. It has an impact on data confidentiality and, eventually, the organisation. Encrypted data makes it impossible for an attacker to use it even if it is stolen [46].

3.2 Data Loss

One issue with data cloud computing security is data loss. Data loss, which can be caused by Accidental Destruction, Viruses, System Faults, or Hacking, is simply the complete erasure of data [46].

3.3 Traffic Hijacking

One of the major risks that end users encounter while using cloud computing is traffic hijacking. It was identified as the third-most serious threat to cloud security in 2013 by Cloud Security Alliance. Hackers typically steal a user's security credentials in this form of assault and claim illegal access to the user's data. An attacker is then able to view all of a user's activities, along with any private cloud transactions they may have [47].

3.4 Crypto-Jacking

The attacker has the ability to control and rule the cloud network by penetrating endpoints and taking advantage of web browsers. This function is efficiently facilitated by crypto-jacking. It helps with operation when there is a probability that there may be a security flaw and the cloud's architecture is at risk. Risk increases the possibility that a device will be compromised for cryptocurrency mining while the user is unaware.

Since it is legal to mine cryptocurrencies, many fraudsters take advantage of the resources. As a result, one can see rising electricity prices, decreased battery capacity, and many other things. We can earn a lot of money by mining cryptocurrencies legally.

3.5 Revenue Loss

In addition to losing their customer base, businesses may also incur losses. Confidential data disclosures could cause damages for clients and enterprises. The sector must employ technology and resources to address the current issue and enhance the updating system. The costs should be applied to pay for both marketing The costs should be applied to both marketing initiatives and legal measures [8].

3.6 Insider Attack

When a corporation hires someone, they will thoroughly investigate that person, especially if that person is an IT professional because the most successful attack that anyone can predict will originate within the business. An Ex-employee or not fully protected employee who seeks to exploit data or services for money or evil intentions is often the insider [48]. It is quite challenging to distinguish between different assaults or privileged insider operations because of the Multitenancy of the cloud computing domain [49].

3.7 Worm Attacks

The goal of a cloud worm injection attack is to disrupt the service being provided, the virtual machine, or the remote application by introducing computer viruses into the cloud architecture [50]. When the identity is recognized, signature-based antivirus can identify threats with high degree of accuracy; but, if the threat entirely changes its signature, the calculation becomes too challenging [51 - 52].

3.8 Distributed Denial of Service (DDoS) Attacks

Cloud Infrastructure, Service hijacking type of attacks are not as destructive as the malicious attacks: Exploiting software flaws, frauds and phishing which gives hackers the added advantage [53]. There are three primary components that carry out DDOS assaults:

- Master: The hacker who attacks using the different types of compromised machines.
- Slave: System that has been compromised, and the attack is carried out using it.
- Victim: This one will be the target of an attack

HTTP-Based DDoS Attack: The Hyper Text Transfer Protocol (HTTP) client communicates with an http server via one of its functions i.e. GET or a POST request. GET is

used to retrieve web content, whereas POST is used on forms to submit information from input fields. Flooding is possible in this scenario when the server allots numerous resources in response to a single request, necessitating a somewhat complicated server processing [54].

3.9 Physical Security

The data centres also expose the data to physical interference. A physical security breach could result from cyber attackers breaking into computer servers and altering, seizing, or erasing the data. These issues necessitate manpower, multi-factor authentication, continuous monitoring, and great levels of security, none of which may be possible for those with private cloud security to handle [33].

3.10 Insecure Cloud Data Transmission

Data transmission between public and private clouds exposes this data to vulnerabilities that further leads to surveillance or cyberattacks. Strong encryption is the best technique to ensure that transmitted data remains secured even if it works as intended [55].

3.11 Supply Chain Risks

When unauthorized agent gets the access to the system through the third party service provider or partner who has the rights to access to system and records, is known as a supply chain assault. As vendors and service providers have more and more access to ever increasing sensitive data of clients, has significantly altered the attack vector on the typical organisation in recent times. While it's possible that security staff are knowledgeable, well-equipped, and follow hybrid cloud sanitation, it can't be assured that allies are in the same position [55].

4. Cloud Security Model

As being physical present is the key component of identity, similarly physical infrastructure security is crucial to establishing effective controls over the organisational infrastructure otherwise, physical access could easily compromise security [56]. An all-encompassing, flexible approach to cloud security is required, one that also takes client needs into account [57]. The prevention and mitigation of risks to information stored in and accessible through cloud services can be helped by a cloud management platform [58].

4.1 Governance, Risk, and Compliance in Security

The organisation's primary duty is to provide organisational structure, processes, and controls so that effective security model for governance, risk management, and compliance can be implemented Any system comprising of technologies, rules & regulations, static or dynamic laws that function within an organisation and provide guidance in order to accomplish a security goal is referred to as governance [59 - 61]. The following are some of the organisation's duties:

- Risk of cloud provider access
- Defend sensitive information and comprehend legal issues
- management of the information life cycle
- Interoperability and portability

An organisation uses service level agreements to ensure that security requirements are followed [62].

4.2 People and Identity Management

- Only authorized users can have access to the assets of the organisation [63].
- Authentication and authorisation use an identity federation model [64].
- For user sign-on, we should rely on single sign-on capabilities.
- Managing identities and properly utilising directory services provides the proper access control.
- Identity management on the web is also an effective choice for identifying the authorized client.

4.3 Application Security

- A secure development process should be used by cloud providers.
- Applications should be protected from external attacks like XML and web service attacks with XML signature and encryption methods [65].

4.4 Information Security

- Attention must be focused on the storage of data, processing, compliance, and auditing [66].
- To guarantee data privacy, a common encryption mechanism and encryption key management should be utilised.
- To address the data/information dilemma, trustworthy virtual domains or policy-based security should be implemented. [67]
- A system for intrusion detection and prevention needs to be created.

4.5 Data Security in Cloud

Resources need new techniques that enable cost-effective administration while ensuring crucial elements like privacy and security as data volume grows. The difficulties are brought on by the dispersal of duties throughout cloud supply chains. A cloud is the most cost-efficient resource.

Many questions are raised by moving the data to the cloud [68]. There are three interconnected layers as shown in Fig. 2 that make up this model. Each layer was given a specific function to increase data security [69]:

- First Layer handles user authentication and issues the user a digital certificate.
- The second layer deals with the data file's encryption for data security.
- The third layer regenerates damaged data more quickly.

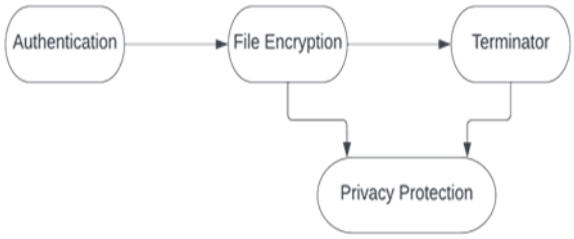

Fig. 2. Three Layers of Cloud Security

Group Key Management (GKM) systems can be used to manage the control of access to cloud data [70 – 72]. The Logical Key Hierarchy (LKH) protocol has been described by the authors in [72].

4.6 Storage Security Method Based on RSA (RSASS)

Remote data is publicly audited using the RSASS approach. It detects server errors, ensures data accuracy, supports dynamic data operations, and enhances performance by cutting down on server computation time. Three parties make up the RSA based storage Security Method (RSASS): Client, Third Party Auditor (TPA), and the Cloud Service Provider. Further, RSASS architecture as depicted in Fig.3 works in two important phases i.e. setup and integration phase [73].

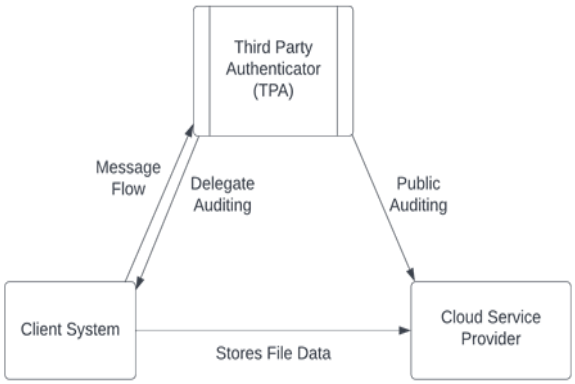

Fig. 3. RSASS Architecture

5. Proposed Cloud Security Model

Encryption Key Card model as proposed in the Fig. 4 will work using the card in a device which will have a private key that is a program which will check and verify with its public key. If it matches, it decrypts the files that you have. The files use AES encryption. You can't decrypt the files without the proper card. Here is how it works:

- The program has a mode where you can run it with an argument. In this mode the program will generate private and public keys. It will store the public keys in your computer and private keys in the pen drive. It also generates a hash of the private key and encrypts the hash and stores it in a file in the card. This hash is the key used in AES encryption.
- When you encrypt a file it will check if the pen drive is the encrypted card and if the keys match. It checks if the keys match by randomly generating a string encrypting it with a public key and decrypting it with the key found in the card. If the decrypted key matches with the generated random string it decrypts the key found in the file used to store hash before and uses that key along with AES to encrypt a file that you want to encrypt.
- While decrypting it uses the same method to check if the keys match. You can also use batch decryption. You can make a text file and name it as "files.txt". If you have a file named files.txt in the pen drive or in the current directory the program will start decrypting the files. This text file should contain the path of the encrypted file in the first line and the path of the new decrypted file as the second line. You can follow this pattern and add as many lines as you want.
- If any of the conditions do not match it won't encrypt/decrypt the file transforming your pen drive to a security key.

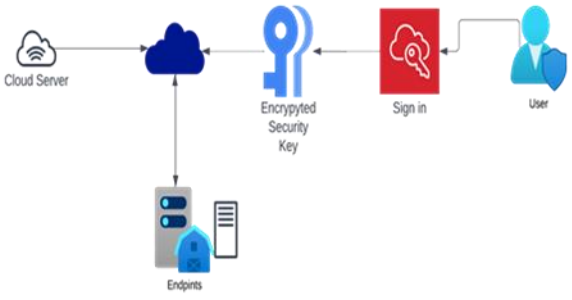

Fig. 4. Encryption Key Card

6. Future Scope

Cloud Computing paradigm consists of the core components (Front end and Back end) for remote computing using virtualization. It includes: client-side applications &

interfaces, web servers and web service providers. Based upon the elaborated studies in the literature survey, still there is scope for the improvement in cloud computing and its security:

- With the advancements in the communication technologies like: 5th generation Internet, IoT (Internet of Things) and Smart cities; Cloud Computing can be implemented more transparently, effectively and efficiently for the remote distributed processing and storage of data.
- With the increasing implementation / use of cloud services in the different fields, extended range of security concerns and vulnerabilities have been exposed by the heterogeneity of enterprise environment.
- Non-transparency about the real–time location of data and work load storage makes it difficult for the reorganization and reduction in the escalation of security concerns.
- Non-transparency in cloud architecture leads to duplication, inability to recognize different types of attacks on time, lack of control over the data access and also the security necessary for meeting regulatory requirements.
- To achieve cloud security effectively both the data and infrastructure must be safeguarded against all types of attacks like: data breaches, hacking of interfaces, use of insecure APIs etc.

Our efforts to address the security issues in a cloud environment are supported by a number of studies. However, many issues that still need to be solved must be addressed in order to provide a secure cloud infrastructure. Traditional problems that exist at the start of cloud computing include those relating to network, data privacy, application, and online service security.

7. Conclusion

Several security concerns with cloud computing were examined in this research. There are several ways to stop each type of attack, but none of them are effective enough to stop them in all circumstances. It is quite difficult to create a system that is completely impervious to any of these serious threats. Discussed were a few potential methods that were put up to address issues with communication security, data anonymization, and data kept in cloud storage. As a result, it was identified that different kinds of algorithms can defend the cloud on various levels and for diverse purposes. It is evident, even the most well-known CSPs, including Google, Amazon and many others, are still dealing with security concerns but are still not at quite a solid point. With all of this degree of technological shortcomings, the only factor that may be used to determine whether to employ cloud technology is the advantages to risk ratio. Both the client as well as cloud host ends must have a thorough knowledge of one another therefore for the cloud to be protected from across all exterior dangers. Data transfer and storage in the cloud are the main goals of cloud computing.

References

[1] S. Vaishali and Pandey S. K., “A Comparative Study of Cloud Security Ontologies”, Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization, India, 2014.

[2] H. Amit and J Karuna Pande, “A Semantic Approach to Cloud Security and Compliance”, IEEE 8th International Conference on Cloud Computing, pp. 1081, 2015

[3] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. Foster, “Virtual Infrastructure Management in Private and Hybrid Clouds”, IEEE Internet Computing, vol. 13, no. 5, pp. 14-22, Sep. 2009.

[4] L. Hsin Tse, K. Chia Hung, W. Po Hsuan and L. Yi Hsuan, “Towards a hosted private cloud storage solution for application service provider”, Proceedings of 2014 International Conference on Cloud Computing and Internet of Things, 2014.

[5] M Armbrust , A Fox , R Griffith , AD Joseph, RH Katz , A Konwinski, G Lee, DA Patterson, A Rabkin, I Stoica and M Zaharia, “Above the Clouds - A Berkeley View of Cloud.”. Technical report UCB/EECS-2009-28, EECS Department, University of Berkeley, California, 2009.

[6] Ling Zheng; Yanxiang Hu; Chaoran Yang, “Design and Research on Private Cloud Computing Architecture to Support Smart Grid”, Third International Conference on Intelligent Human-Machine Systems and Cybernetics, pp. 1, 2011

[7] G. Adam, “The Hybrid Cloud Security Professional”, IEEE Cloud Computing, Volume: 3, Issue: 1 pp. 2, 2016

[8] P. Mell and T. Grance, The NIST Definition of Cloud Computing, Nat’l Inst. of Standards and Technology, pp. 3, 2011.

[9] J. Sathyan and K. Shenoy, "Realizing unified service experience with SaaS on SOA", 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE '08), 2008.

[10] L. Gouling “Research on Independent SaaS Platform”, 2nd IEEE International Conference on Information Management and Engineering, 2010.

[11] D. Rajdeep, R. A. Reddy and K. Dharmesh, “Virtualization vs Containerization to support PaaS” pp-2, 2014.

[12] http://www.eucalyptus.com, February, 2013.

[13] J. Bresnahan, D. LaBissoniere, T. Freeman and K. Keahey,“Cumulus: An Open Source Storage Cloud for

Science", Science Cloud 2011, San Jose, CA. June 2011
[14] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. Foster, "Virtual Infrastructure Management in Private and Hybrid Clouds', IEEE Internet Computing, vol. 13, no. 5, pp. 14-22, Sep. 2009.
[15] http://www.openstack.org, February, 2013.
[16] P. Chandan and D. Surajit, "Cloud Computing Security Analysis: Challenges and Possible Solutions", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016
[17] L. Han, X. Wenjuan and D. Yi, "Research on Building of Electronic Community Based on Cloud Computing"., 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), pp-3, 2011
[18] L. Han, X. Wenjuan and D. Yi, "Research on Building of Electronic Community Based on Cloud Computing"., 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), pp-3, 2011
[19] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, Volume 34, Issue 1, pp, 1-11, Jan 2011.
[20] Ramgovind, S.; Eloff, M.M.; Smith, E., "The management of security in Cloud computing," Information Security for South Africa (ISSA), 2010, vol., no., pp.1,7, 2-4 Aug. 2010.
[21] T. Mather, S.Kumarswamy, S. Latif, "'Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O'Reilly Media, 2009.
[22] P Kamongi, "Nemesis: Automated Architecture for Threat Modeling and Risk Assessment for Cloud Computing", ASE 2014
[23] Popović, K. and Hocenski, Z., "Cloud computing security issues and challenges," MIPRO, 2010 Proceedings of the 33rd International Convention, vol., no., pp.344,349, 24-28 May 2010
[24] NIST, NIST Cloud Computing Reference Architecture, 2011.
[25] Cloud Security Alliance, "The Notorious Nine: Cloud Computing Top Threats in 2013"', p8-p21, 2013.
[26] Mell, P. and Grance, T., "'The NIST Definition of Cloud Computing", (Special Publication 800-145), W3C recommendation, World Wide Web Consortium, 2004.
[27] Jörg Hladjk, "Privacy and Data Protection", Vol 7 Issue 4, IT compliance and IT Security-Part 1, p 987-997, 2017.
[28] Gordin, A. Graur, A. Potorac and D. Balan, "Security Assessment of OpenStack cloud using outside and inside software tools", International Conference on Development and Application Systems, pp. 170-174, 2018.
[29] V.A. Jujare, "Cloud computing: Approach, Structure and Security" In Second International Conference on Computing Methodologies & Communications, 2021.
[30] K. Raj, "Research on Cloud Computing Security Threats using Data Transmission" International Journal of Advanced Research in Computer Science and Software Engineering, India Volume 5, Issue 1, pp. 399-402, Jan 2015.
[31] Bashir SF and, Haider S., "Security threats in cloud computing", Proceedings of the International Conference for Internet Technology and Secured Transactions, pp 214–219, 2011
[32] J. Orea, "Quick guide to the reference architecture: Trusted Cloud Initiative", Cloud Security Alliance, 2011.
[33] T. Hamed and R. Marjan Kuchaki, "A survey on security challenges in cloud computing: issues, threats, and solutions", The Journal of Supercomputing, Volume 76, 9493–9532, pp. 9508, 2020.
[34] F. Liu, "NIST Cloud Computing Reference Architecture", National Institute of Standards and Technology, U.S Department of Commerce, Special Publication 500-292, Sep. 2011.
[35] R. Roman, J. Lopez and M. Mambo, "Mobile Edge Computing: a survey and analysis of security threats and challenges", Future Generation Comput Syst 78:680–698, 2018.
[36] GICTF, "Use cases and functional requirements for inter-Cloud computing", GICTF White Paper, Global Inter-Cloud Technology Forum, 2010.
[37] Celesti, F. Tusa, M. Villari and A. Puliafito, "How to Enhance Cloud architectures to enable cross-federation", Cloud Computing (Cloud), IEEE 3rd International Conference on, Seiten 337 – 345, 2010.
[38] H. Takabi and J. Joshi, "Security and Privacy Challenges in Cloud Computing Environments", IEEE, 2011.
[39] Salasiah and A. B. Khairul Azmir, "Toward Cloud Computing Reference Architecture", Cyber Resilience Conference (CRC), 2018
[40] Yanuarizki, L. Charles, I. Heru Purnomo and J. Arkav "Toward Cloud Computing Reference Architecture: Cloud Service Management Perspective", International Conference on ICT for Smart Society, 2013.
[41] J. Hurwitz, "Understanding IT Governance in Cloud Computing", http://www.dummies.com/howto/content/understanding-it-governance -in-cloudcomputing.html.
[42] Security Issues in Cloud Computing https://www.jigsawacademy.com/blogs/cloud-computing/security-issues-in-cloud-computing.

[43] Y. Wei, Y. F. Lian and D. G. Feng, "A network security situational awareness model based on information fusion [J]", Journal of computer research and development, vol. 46, no. 3, pp. 353-362, 2009.

[44] Cloud Computing – A Practical Approach by Velte, Tata McGraw Hill Edition (ISBN-13:978-0-07-068351-8).

[45] D. Wesam, T. Ibrahim and M. Christoph, "Infrastructure as a Service Security: Challenges and Solutions," 7th International Conference on Informatics and Systems, pp. 1-8, 2010.

[46] R. Kalaiprasath, R.Elankavi and R. Udayakumar, "Cloud Security and Compliance- A Semantic Approach In End To End Security " International Journal On Smart Sensing and Intelligent Systems Special Issue, pp-486, 2017.

[47] K. Abhirup and Sarishma, "Mobile Cloud Computing: Principles and Paradigms" IK International Conference on Cloud Computing, 2015.

[48] J. Jomina and N. Jasmine, "Major Vulnerabilities and Their Prevention Methods in Cloud Computing", Proceedings of ICBDCC18, Jan, 2019.

[49] Duncan, S. Creese and M. Goldsmith, "Insider attacks in cloud computing" IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[50] Bisong, and Rahman M. "An overview of the security concerns in enterprise cloud computing", Int. J. Netw. Secur. Appl. (IJNSA) 3(1), Jan 2011.

[51] Yang, Z., Qin, X., Yang, Y. and Yagnik. T. "A hybrid trust service architecture for cloud computing" International Conference on Computer Sciences and Applications, 2013.

[52] S.M. Habib, S. Hauke, S. Ries and M. Muhlhauser, "Trust as a facilitator in cloud computing: A survey", J. Cloud Comput. Adv. Syst. Appl., 2012.

[53] ISACA (auditor's perspective journal) http://www.isaca.org/Journal/Past-Issues/2009/Volume-6/Pages/ Cloud-Computing-An-Auditor-s-Perspective1.aspx

[54] J. Rameshbabu, B. Sam Balaji, R. Wesley Daniel and K. Malathi, "A prevention of DDoS attacks in cloud using NEIF techniques" Int. J. Sci. Res. Publ. 4(4) ISSN 2250-3153, 2014.

[55] Top 4 Hybrid Cloud Security Challenges (xmcyber.com) "https://www.xmcyber.com/blog/top-4-hybrid-cloud-security-challenges/#:~:text=Top%204%20Hybrid%20Cloud%20Security%20Challenges%201%201.,Compliance%20...%204%204.%20Supply%20Chain%20Risks%20"

[56] S. Fawaz, Al-Anzi;, Y. Sumit Kr. and S. Jyoti, "Cloud computing: Security model comprising governance, risk management and compliance", International Conference on Data Mining and Intelligent Computing, Sep, 2014.

[57] B. Michael and G.Andrzej, "Toward a Framework for Cloud Security, Algorithms and Architectures for Parallel Processing", Volume 6082/2010, pp. 254-263, 2010.

[58] 4 Emerging Public Cloud Security Challenges to Watch For https://cloudcheckr.com/cloud-security/emerging-public-cloud-security-challenges.

[59] T. Mather, S. Kumaraswamy and S. Latif, "Cloud Security and Privacy", O'Reilly Media, Inc., Sebastopol, CA, 2009.

[60] S. Ghemawat, H. Gobioff and S. Leung, "The Google file system, " Proceedings of the 19th Symposium on Operating Systems Principles, pp. 29-43, 2003.

[61] Eludiora and Safiriyu, "A User Identity Management Protocol for Cloud Computing Paradigm" International Journal of Communications, Network & System Sciences, 2011.

[62] P. Brereton, BA. Kitchenham, D. Budgen, M. Turner and M. Khalil "Lessons from applying the systematic literature review process within the software engineering domain". J Syst Softw 80(4): 571-583, 2007

[63] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing", SIAM Journal on Computing, vol. 32, no. 3, pp. 586-615, 2003.

[64] M. R. Momeni, "A lightweight authentication scheme for mobile cloud computing", International Journal of Computer Science and Business Informatics, vol. 14, no. 2, 2014.

[65] M. Koji, "XML Signature/Encrption – the Basis of Web Services Security", NEC Journal of Advanced Technology, vol. 2, no. 1, 2005.

[66] H. Jay and N. Mark, "Assessing the Security Risks of Cloud computing[EB/cL]", Garmer Technology Business Research In—sight, 2008.

[67] W. Li, L. Ping, "Trust model to enhance Security and interoperability of Cloud environment", Proceedings of the 1st International conference on Cloud Computing. Springer Berlin Heidelberg, Beijing, China, pp 69-79, 2009.

[68] R. Yenumula, "Big Data Security in Cloud Environment", IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), pp. 103, 2018

[69] H. Shital A. and M. Sunil B, "An Analysis on Data Accountability and Security in Cloud", International Conference on Industrial Instrumentation and Control (ICIC) College of Engineering Pune, India. May 28-30, pp. 715, 2015.

[70] S. Ramgovind and E. Smith, "The Management of Security in Cloud Computing", IEEE Information Security for South Africa (ISSA), 2010.

[71] Z. Dimitrios and L. Dimitrios, "Addressing cloud computing security issues", Future Generation Computer Systems, vol. 28, pp. 583-592, 2012.

[72] D. Wallner, E. Harder and R. Agee, "Key Management for Multicast: Issues and Architectures", RFC, vol. 2627, June 1999.

[73] M. Venkatesh, Sumalatha and C. Selva Kumar, “Improving Public Auditability Data Possession in Data Storage Security for Cloud Computing”, ISBN 978-1-4673-1601-9/12, 2012.