**Adopting Information Security Techniques for Cloud Computing–A Survey**

**Abstract**

* Popularly used encryption techniques that is helpful to secure sensitive information on cloud.
* Diverse versions of the encryption techniques surveyed and analyzed to identify optimization features for cloud security.

**Keywords** — Cloud Computing; cloud security; data privacy; encryption techniques.

**Introduction**

* Its main goal is secure and quick data storage for sensitive information
* factor of risk i.e. data security and privacy protection of sensitive data, authentication of user, access control, application security
* Data security is among the challenges that will increase great concerns for the user when a person stores sensitive information on the cloud servers.
* Three major concerns are involved within the cloud computing:

1. Move the personal sensitive data to the cloud servers.
2. Move data from cloud servers to the client’s or customer’s computer and
3. To store customer’s personal information in cloud server is known as remote server (not owned by the customers).

**Literature Review**

1. A Strong User Authentication Framework for Cloud Computing - proposed on 2 step authentication issue where the user verified before entering the cloud
2. Identity-based Authentication for Cloud Computing - combination of Identity-based Hierarchical Model and corresponding encryption and signature. After simulation, it is conclude that it protocol is more efficient and lightweight than other protocols.
3. New Approaches to Security and Availability to Cloud Computing - proposed the framework that secure cloud data by integrity and verification for data availability. another issue in public clouds is availability and reliability assurances
4. Secure Cloud Computing Benefits, Risks and Controls - focused easing for cloud security risk as a compulsory step to ensure secure cloud environment. It provided an overview about the cloud computing security risks
5. Data Security and Privacy Protection Issues in Cloud Computing - The most fundamental challenges are access control and separation of sensitive data. This paper proposed different techniques to ensure access i.e. fine-grained access authorization.
6. Cryptographic Cloud Storage - proposes a cryptographic plan for secure management of data by using the ID based cryptography. unauthorized client cannot get the information without the owner's permission
7. "Efficient cloud storage confidentiality to ensure data security - Encryption with obscurity; both concepts are exclusive for securing information in storage management. Applying encryption and muddling systems on the cloud information will give more assurance against unapproved usage of data.
8. Data authentication and integrity verification techniques for trusted/untrusted cloud servers-- Advance message based confirmation process is defined. It is the process only approved users can have access to data by identifying his/her identity using message uprightness.
9. Security storage in the Cloud Computing: A RSA-based assumption data integrity check without original data
10. Enhanced cloud computing security and integrity verification via novel encryption techniques -- Three stages (public, private and hybrid ) - Some encryption techniques are implemented on these three stages to cover areas regarding security factor.

Hybrid - Two tier security structural arrangement, Public - Decoding and encryption techniques, Private - token era instrument

1. “A new RBAC based access control model for cloud computing-- This model incorporates two sort of parts, client part (UR) and proprietor part (OR)
2. Cloud Hooks: Security and Privacy Issues in Cloud Computing-- explored key issues, which had long-term importance in cloud hooks (security and privacy issues)
3. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing - proposed a hybrid technique i.e. attribute-based encryption, proxy encryption and lazy re-encryption. These hybrid method, after analysis, proved to be highly efficient and secure. This technique is highly useful against fine-grained data access control.

**ANALYSIS**

* From analyzing chosen 12 parameters

User Authentication, Data Confidentiality, Privacy protection ,Data Security , Non-repudiation , Data Integrity , Availability of data and services , Data Control ,Access control , Methodology ,Data encryption ,efficiency

**CONCLUSION**

* It main goal a secure and quick data storage for sensitive information.
* User authentication and control access is still a highlighted factor in cloud computing.
* data confidentiality is an important feature of cloud computing. to secure them encryption techniques. Encryption is not so powerful to secure so more paper proposes encryption with obscurity

**FUTURE WORK**

This security problem can be resolve by applying different encryption techniques to cloud computing. Confusion and diffusion need to be kept strong when choosing the encryption techniques

**An Analysis of the Cloud Computing Security Problem**

**Abstract**

* model architecture, multi-tenancy, elasticity, and layers dependency stack.
* investigated the problem from the cloud architecture perspective, the cloud offered characteristics perspective, the cloud stakeholders’ perspective, and the cloud service delivery models perspective.

**Keywords**: cloud computing; cloud computing security; cloud computing security management.

**INTRODUCTION**

* Definition : “a model for enabling convenient, on-demand 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. ”.
* Multitenancy and elasticity
* **Both characteristics focus on improving resource utilization, cost and service availability.**
* Vendor lock-in, multi-tenancy and isolation, data management, service portability, elasticity engines, SLA management, and cloud security are well known open research problems in the cloud computing model.
* We group these issues into architecture-related issues, service delivery model-related issues, cloud characteristic-related issues, and cloud stakeholder-related issues.

**LITERATURE REVIEW**

1. Cloud Computing Use Cases Version 3.0 - They consider use cases from different perspectives including customers, developers and security engineers.
2. Cloud computing: benefits, risks and recommendations for information security- discussed security risks - the risks likelihood, impacts, and vulnerabilities
3. Cloud security issues - security SLA’s specifications
4. "Cloud computing security issues and challenges - data integrity, payment, and privacy of sensitive information - security management standards such as ITIL, ISO/IEC 27001 and Open Virtualization Format (OVF).
5. On Technical Security Issues in Cloud Computing - computing model such as XML-attacks, Browsers’ related attacks, and flooding attacks.
6. Understanding Cloud-Computing Vulnerabilities : technology-related, cloud characteristics -related, security controls- related.

**THE CLOUD COMPUTING ARCHITECTURE AND SECURITY IMPLICATIONS**

* Private , public and hybrid
* Services ( IAAS , SAAS , PAAS )

**CLOUD COMPUTING CHARACTERISTICS AND SECURITY IMPLICATIONS**

* Two key characteristics: **multitenancy**  and **elasticity** . Both characteristics turn out to have serious implications on the cloud model security
* .**Multitenancy**

1. Approach 1 : each tenant - dedicated instance - own customization
2. Approach 2 : each tenant - dedicated instance - different configuration
3. Approach 3 : all tenant - same - run time configuration
4. Approach 4 : tenants directed - load balancer - redirects - suitable instance based on current instances load.

* Secure multitenancy - isolation and location transparency
* IAAS - isolation should consider VMs’ storage, processing, memory, cache memories, and networks
* PAAS - isolation among running services and APIs’ calls
* SAAS - isolate among transactions carried out on the same instance by different tenants and tenants’ data.

**CLOUD COMPUTING ’S DEEP DEPENDENNCIES STACK**

* IAAS - cloud physical infrastructure layer ,virtualization layer ,virtualized resources layer
* PAAS - platform layers, APIs and Services layers
* SAAS - applications and services

**CLOUD COMPUTING STAKEHOLDERS AND SECURITY IMPLICATIONS**

* Stakeholders ( cloud provider , service provider and service consumers )
* Security SLA management frameworks Moreover, SLAs are high level contracts where the details of the security policies and security control and how to change at runtime are not included.
* cloud providers are not able to deliver efficient and effective security controls because they are not aware of the hosted services’ architectures

**CLOUD COMPUTING SERVICE DELIVERY MODELS AND SECURITY IMPLICATIONS**

* IAAS issues

VM security, Securing VM images repository, Virtual network security, Securing VM boundaries , Hypervisor security

* PAAS issues

SOA related security issues ( DOS attacks, Man-in-the-middle attacks, XML-related attacks, Replay attacks, Dictionary attacks, Injection attacks and input validation related attacks ) , API Security

* SAAS issues

Web application vulnerability scanning , Web application security misconfiguration and breaking

* Cloud Management Security Issues

CML component include SLA management, service monitoring, billing, elasticity, IaaS, PaaS, SaaS services registry, and security management of the cloud.

**CLOUD COMPUTING SECURITY ENABLERS**

1. Identity & Access Management (IAM) and Federation

It should include: Identity Provisioning and de-provisioning, identity information privacy, identity linking, identity mapping, identity federation, identity attributes federation, single sign on, authentication and authorization. Such system should adopt

existing standards, such as SPML, SAML, OAuth, and XACML , to securely federate identities among interacting entities within different domains and cloud platforms

2. SDLC 3. Key Management 4. Security Management 5. Secure Software Development Lifecycle 6. Federation of security among multi-clouds

**CONCLUSION**

we can summarize the cloud security problem as follows:

• Some of the security problems are inherited from the used technologies such as virtualization and SOA.

• Multi-tenancy and isolation is a major dimension in the cloud security problem that requires a vertical solution from the SaaS layer down to physical infrastructure (to develop physical alike boundaries among tenants instead of virtual boundaries currently applied).

• Security management is very critical to control and manage this number of requirements and controls.

• The cloud model should have a holistic security wrapper, as shown in figure 3 , such that any access to any object of the cloud platform should pass through security components first.

Based on this discussion we recommend that cloud computing security solutions should:

• Focus on the problem abstraction, using model-based approaches to capture different security views and link such views in a holistic cloud security model.

• Inherent in the cloud architecture. Where delivered mechanisms (such as elasticity engines) and APIs should provide flexible security interfaces.

• Support for: multi-tenancy where each user can see only his security configurations, elasticity, to scale up and down based on the current context.

• Support integration and coordination with other security controls at different layers to deliver integrated security.

• Be adaptive to meet continuous environment changes and stakeholders needs.

**FUTURE WORK**

To be able to resolve such problem we need to:

1. Capture different stakeholders security requirements from different perspectives and different levels of details;
2. Map security cloud architecture, security patterns and security enforcement mechanisms;
3. Deliver feedback about the current security status to the cloud providers and consumers

* **Adaptive model-based approach**

Models will help in the problem abstraction and the capturing of security requirements of different stakeholders at different levels of details. Adaptive-ness will help in delivering an integrated, dynamic and enforceable cloud security model. The feedback loop will measure the security status to help improving the current cloud security model and keeping cloud consumers aware with their assets’ security status (applying the trust but verify concept).

**Security Threats in Cloud Computing**

**Abstract**

**Keyword**: Cloud Computing; Cloud Computing Security; Security Survey of Cloud Computing; Security threats; Secure Cloud computing

**INTRODUCTION**

* zero maintenance cost is involved since the service provider is responsible for the availability of services and clients are free from maintenance and management problems of the resource machines
* SAAS ,PAAS ,IAAS

**LITERATURE REVIEW**

1. Towards a Data-centric View of Cloud Security :

* data centric view of cloud security.
* security platform for cloud computing, which is named as Declarative Secure Distributed Systems (DS2).
* Secure Network Data log (SeNDlog)

1. Transparent Security for Cloud : Transparent Cloud Protection System (TCPS) for improved security of cloud services
2. data privacy issues - data protection framework. Their proposed framework comprises of three key components: policy ranking, policy integration and policy enforcement

**CRITICAL EVALUATION**

1. Secure Provenance in Cloud Computing - Bilinear pairing method
2. Trust cloud computing - Trusted Cloud Computing Platform (TCCP)
3. Implementation and research issues in cloud computing - Virtual Computing Laboratory (VCL)
4. Data- centric cloud security - DS2 platform
5. Security audit in public infrastructure Clouds - Amazon EC2

Transparent Cloud Security - Transparent cloud protection system TCPS

**FUTURE WORK**

**CONCLUSION**

**Efficient Cloud Storage Confidentiality to Ensure Data Security**

**Abstract**

* Cloud storage is efficient for data storage
* **Encryption and obfuscation** as two different techniques to protect the data in the cloud storage.
* **Encryption** is the process of converting the readable text into unreadable form using an algorithm and a key. Obfuscation is same like encryption.
* **Obfuscation** is a process which disguises illegal users by implementing a particular mathematical function or using programming techniques.
* Encryption can be applied to alphabets and alphanumeric type of data and obfuscation can be applied to a numeric type of data.

**Keywords**: - Cloud Storage; Data Protection; Confidentiality ;Encryption; Obfuscation;

**INTRODUCTION**

* The cloud storage is implemented using cloud computing that means utilizing the software and hardware resources of the cloud computing service provider.
* Data protection is concerned with data confidentiality, integrity, authentication, availability and so on.
* Confidentiality could be used to protect the data from outsiders as well as insiders attack.

**DATABASE MANAGEMENT IN THE CLOUD**

* Cloud database management system : delivers computing resources as a service instead of a product

**RELATED WORK**

1. A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems : Control Access Data Storage (CADS) that included the necessary policies, processes and control activities for the delivery of each of the Data service offerings
2. “Data Storage Security in Cloud using Metadata : In this model, the time required for generating the cipher key is proportional to the number of attributes in the metadata as well the algorithms used for cipher key generation.

Two novel features

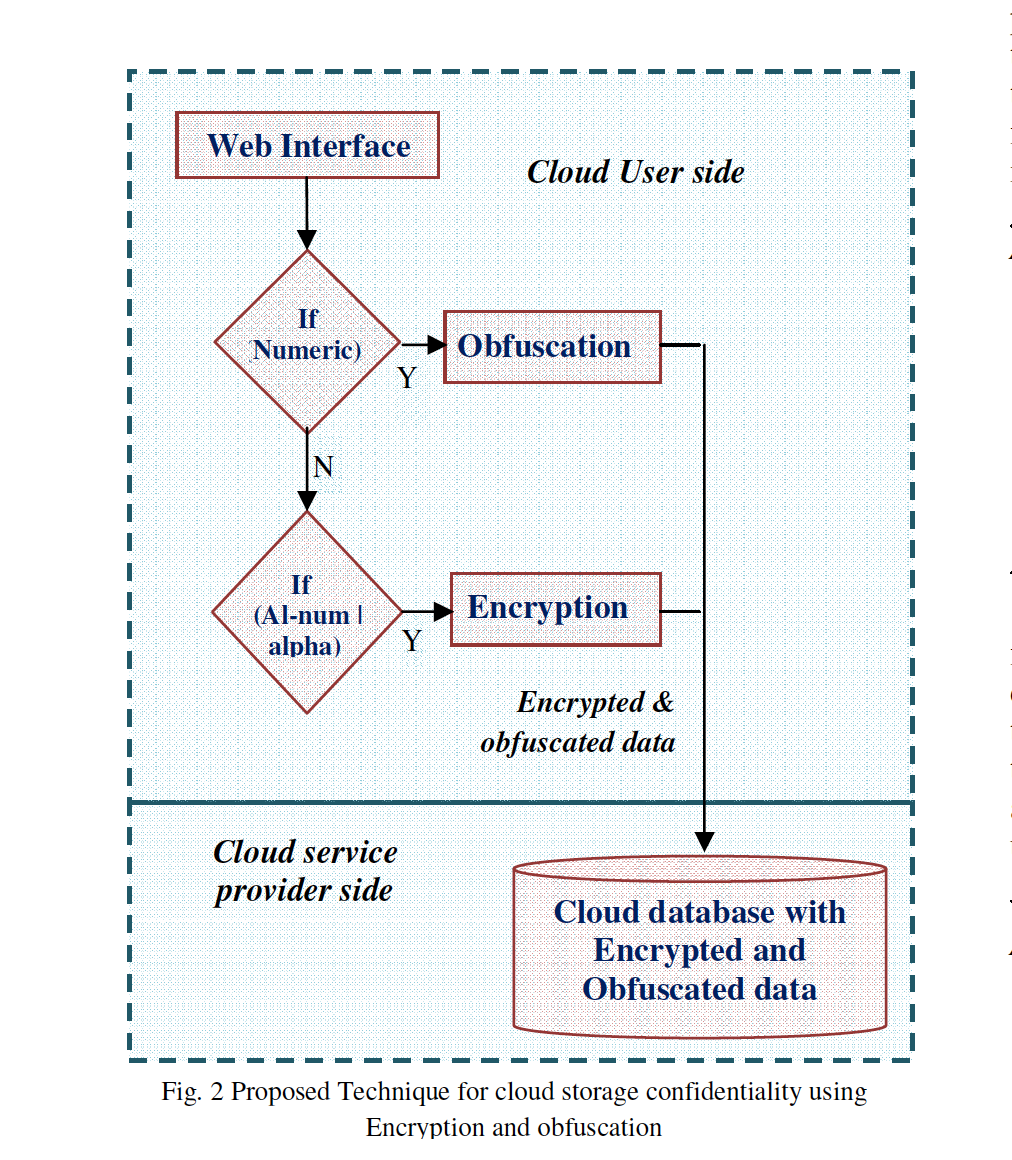
* Security is provided by the proposed design, where the encryption and decryption keys cannot be compromised without the involvement of data owner and the metadata data server (MDS).
* The cipher key generated using the modified feistel network holds good for the avalanche effect as each round of the feistel function depends on the previous round value. This approach is time consuming for generation cipher key

1. “CP-ABE Based Encryption for Secured Cloud Storage Access: Especially, cipher text-policy attribute based encryption (CP-ABE) enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the cipher text, and enforce it on the contents. Thus, each user with a different set of attributes is allowed to decrypt several pieces of data per the security policy.

**CLOUD STORAGE ISSUES**

* Trust, Cloud Service provider agreements, Data history , Data Possession

**PROPOSED CONFIDENTIALLY TECHNIQUE**



* Obfuscation is a technique by applying through specific mathematical functions or by using programming techniques.

**Algorithm#1** is used to find out the type of data (T) which is ready to store in the cloud storage. Based on the type of data, encryption or obfuscation is applied on the data before forwarded to the cloud. If the data (T) are digits, then obfuscation technique is applied, if the data are alphabets or alphanumeric then encryption is applied on the data. This algorithm will call the corresponding algorithm based on the data type of (T).

**Algorithm#2** is used for obfuscation. This algorithm is used for numeric data type. Obfuscation is a technique by applying through specific mathematical functions or by using programming techniques. This algorithm doesn’t use any key to mask the user’s data. There is no. of obfuscation related techniques are available. This paper uses two mathematical function namely root () and floor () functions. These two mathematical functions applied to the data to obfuscate them.

**Algorithm#3** is used for encryption. This algorithm is used for numeric or alphanumeric data type. This is a symmetric encryption algorithm. The algorithm uses substitution and transposition technique to convert the plain text into cipher text. ASCII codes of the plain text are used throughout the algorithm. It uses four keys for encryption, and same keys are used for decryption also.

**CONCLUSION**

* Encrypted data are stored on storage servers while secret key(s) are retained by data owner;
* obfuscation technique is used to increase the confidentiality of data.
* The user data are encrypted or obfuscated before they are forwarded to the cloud storage

**Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm**

**Abstract**

* Security and privacy are the key issues for cloud storage.

**Keywords**: Cloud Storage, Security, Privacy, Encryption Algorithm, Cryptography

**INTRODUCTION**

* Virtualization is the core concept supported in the cloud computing.
* virtual machine images can be restarted in a different location to provide for disaster recovery
* Insider as an administrator can have the possibility to hack the user‟s data
* Cryptography is a technique applied for encryption and decryption.
* Conventional ( Same key is used for encryption and decryption and public ( Separate keys are used for encryption and decryption ) key Cryptography

**ISSUES IN CLOUD DATA STORAGE**

* Privacy
* Trust → whether there is unauthorized secondary usage of PII ( Personally Identifiable Information)
* Uncertainty, i.e. ensuring that data has been properly destroyed by the one who controls retention of data on how the privacy breaches have occurred and how the fault is determined in such cases
* Compliance, i.e. environments with data proliferation and global, dynamic flows, and addressing the difficulty in complying with transborder data flow requirements.
* Security
* Many clients worry on the vulnerability of remote data to hackers
* Ownership
* Performance and Availability
* Long-term Viability
* Data backup
* Many providers are now offering data dumps onto media or allowing users to back up data through regular downloads.

**CLASSICAL ENCRYPTION**

* two general principles namely **substitution cipher** and **transposition cipher**

1. Caesar Cipher , Playfair Cipher, Vigenere Cipher, Rail fence technique

**PROPOSED ALGORITHM**

* integrating substitution cipher and transposition cipher.
* initially the plaintext is converted into corresponding ASCII code value of each alphabet.
* key value range between 1 to 256.

“ algo are discussed in this paper if you want please go through ”

**CONCLUSION**

* Cryptographic techniques are used to provide secure communication between the user and the cloud.
* Symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data in cloud storage.
* Since the user has no control over the data once their session is logged out, the encryption key acts as the primary authentication for the User.
* By applying this encryption algorithm, user ensures that the data is stored only on secured storage and it cannot be accessed by administrators or intruders.