TABLE OF CONTENTS

1. Abstract

The adoption of cloud computing has significantly increased in the past couple of years. The replacement of physical entities with the cloud entities using virtualization has improved flexibility, scalability and performance in terms of computing. However, with the increased usage of cloud computing, security in cloud has become a huge issue. There has been considerable increase in the vulnerabilities related to the cloud infrastructure. The potential hackers have gained advanced skills to compromise data in the cloud. With the current threat posed by hackers, it is crucial to have new advanced methodologies and models for security in cloud. The proposed report analyses the existing methodologies regarding cloud security and suggests a novel security framework with the implementation of three step authentication process, encryption techniques, file fragmentation and replication and deployment of honeypot system for securing the database servers of the cloud architecture. This proposed framework can be used for securing sensitive data in the cloud. Section 2 of this report discusses the Research Significance. Section 3 of this report discusses the existing approaches in cloud security, Section 4 of this report critically analyses the existing approaches , Section 5 of the report contains the proposed framework, section 6 is the conclusion and section 7 is the references used in the report.

Keywords: authentication, encryption, fragmentation and replication, honeypot, Cloud Security Threats

2. Research Significance

Cloud computing is the delivery of computing resources such as storage, databases, applications, networks, and services to users over the internet. These services can be provisioned as and when required and released upon completion of usage. Cloud service providers offer businesses and individual customers with the optionality of leasing these services either for a specific period or as a pay-as-you-use service. The introduction of this technology has the potential to transform the way businesses function by providing them with simple and rapid provisioning of required services, scalability and flexibility at a reasonable cost (Carroll, Merwe & Kotze 2011).As per Columbus (2018),around 77% of organisations worldwide contain at least one application or a part of their company's computing infrastructure on the cloud. Therefore, it can be inferred that most enterprises are moving towards adopting cloud computing services.

The conventional methodology of implementing computational resources involved setting up and management of applications, data, operating systems, servers, virtualisation, storage and networking by an individual organization. Cloud computing provides the following types of services which simplifies the process of planning and implementing computing services.

1) **Infrastructure-as-a-service (IaaS)**– With IaaS, the cloud service provider handles the servers, virtualization, storage, and networking for an organization. However, the client is responsible for the management of applications, data and operating systems. Therefore, IaaS service providers are responsible for managing the underlying hardware that supports data applications. Examples of IaaS service providers include companies like Amazon, IBM and Google.
2) **Platform-as-a-service (PaaS)** – With PaaS, the cloud service provider is responsible for managing the operating system, servers, virtualization, storage and networking for an organization. However, the client is responsible for handling applications and data. Examples of PaaS service providers include Microsoft Windows Azure, Google Application Engine and Force.com.
3) **Software-as-a-service (SaaS)** – With SaaS, the cloud service providers are responsible for the management of the entire IT infrastructure including applications, data,operating system, servers, virtualization, storage and networking for an organization.Therefore,the service providers offer a range of business applications which can be utilised by the client over the internet for day-to-day business operations. Examples of SaaS providers include Salesforce.com, Drobox and Apple iCloud.

One of the key features of cloud computing services is Multi-tenancy. Multi-tenancy refers to sharing of the service providers resources to store applications and other data. This means, an organization may have their website hosted alongside other organizations on the same server. This is especially the case when the organization opts for a public cloud infrastructure. On the contrary, Private clouds usually involve a single enterprise having dedicated resources to store their data. Therefore, only individuals from the enterprise can access the private cloud.

Cloud service providers offer enterprises with numerous ways of implementing their cloud services, architectures and models along with various types of technologies and applications hosted on them. With the hardware, software and applications hosted and managed by the cloud service providers, security becomes a key concern for enterprises that adopt these services. Maintaining security by ensuring the integrity, confidentiality and reliability of customers data is

one of the key responsibilities of cloud service providers. The cloud service providers also need to ensure that the location of customer data is protected. Therefore, Service providers need to have security mechanisms which not only provide protection to customer data and resources but also provide protection from external attacks.

Security concerns surrounding the cloud environment is one of the major challenges which hampers the acceptance and distribution of cloud technology(Aljumah & Ahanger 2020).This section of the report discusses the various security threats surrounding cloud computing technology and how these issues impact enterprises adopting the technology.

Security threats in Cloud computing

Cloud computing technology is associated with the following security threats:

1) **Data Breaches:**

   Cloud service providers handle data from numerous individuals and organisations. Therefore, the data that is stored, analysed and shared in the cloud environment is of extremely high value. A data breach is an incident where data is intentionally or unintentionally exposed or made available to an unauthorised user. A data breach in the cloud environment can occur when confidential data is viewed, copied, transferred or stolen by an individual who is unauthorised to do so. When a data breach occurs in an organization that stores and manages its own data, the organization handles the incident with utmost priority keeping its own interests in mind. However, a data breach in a cloud environment may expose more than a single organizations data. Therefore, Cloud service providers need specific mechanisms or protocols in place to ensure customer data is protected and there are specific defence mechanisms to handle such breaches. Data breaches usually occur due to various factors such as human error, targeted attacks, vulnerabilities associated with the cloud infrastructure or applications and shortcomings associated with existing security policies with relation to detection of threats, mitigation, security intelligence and so forth. Facebook which is a social-media giant went through a massive data breach, compromising around 540 million records of its users in Early 2019(Pedigo 2019). Facebook offers third party applications which do not operate with the same security policies and standards and hence introducing the threat of exposing shared data if left on servers that are not secured properly. The security breach occurred because a Mexican company named “CulturaColectiva” exposed around 540 million records of Facebook users by storing the shared data on an unsecure AWS Server. These records

contained information linking Facebook users with their profiles, comments and likes. Therefore, protection against data breaches can be achieved by ensuring that appropriate security policies are implemented by both cloud service providers and organizations utilising these services.

2) **Data Loss:**

Loss of data is another key issue with relation to cloud security. Data loss is a sensitive issue for any organization and can have devastating impacts on their business. In the cloud environment, it refers to the deletion and alteration of the original data. They usually occur due to faults in the data storage system, malicious attacks, compromised encryption keys, human error, power failure and hardware failure. Data losses could also occur due to events such as natural disasters or physical destruction of the associated data centres. In June 2012, A data centre which was owned by Amazon and hosted the amazon web services was destroyed by a powerful storm denying availability of data for major companies like Netflix, Instagram and Pinterest for around six hours(Kleyman 2015). Data loss is a major issue for cloud service providers as it may result in customers losing trust and moving their business elsewhere. Therefore, cloud service providers need to ensure appropriate mechanisms are established in order to protect the loss of data. Organizations utilising the cloud services should also ensure their data is being backed up and monitored in the cloud environment.

3) **Account/Service Hijacking:**

Account/Service Hijacking involves an unauthorised user obtaining credentials of a legitimate user in order to gain access to their account, data or other services. This threat impacts the privacy of the users as the attacker can gain access to the users' data and make modifications or delete data, monitor activities and even redirect network traffic. Therefore, Account/Service hijacking compromises an organisations cloud environment. Network attacks such as Cross Site Scripting (XSS), phishing, man-in-the-middle attack, buffer overflow attack, malware invasion result in Service or account hijacking. A famous case of account hijacking is the attack on the New York Times website by a Syrian hackers' group in 2013.The hackers gained access to the credentials of a reseller associated with Melbourne IT and used these credentials to send out a phishing email notifying the recipients to change their passwords. Melbourne IT is an Australian based domain registrar

organisation. The attackers logged the password changes and were eventually able to access and modify the DNS related information associated with the New York Times website. Any user attempting to access the New York Times website was redirected to a Syrian website displaying political information. The incident resulted in the New York Times website being down for almost six hours (Tirumala & Hira 2015)

4) **Denial of Service Attacks (DOS):**

Denial of Service attacks results in legitimate users being unable to access the cloud network, data, storage, and other computational resources. The attack is usually carried out by compromising an existing service or introducing additional traffic to consume the cloud network resources such as network bandwidth, memory and computational power. Distributed Denial of Service attacks(DDOS) is a type of Denial of service attack where multiple network resources are compromised and utilised by attackers to introduce additional traffic in the cloud which either causes a delay in cloud operations or denial of cloud services to its legitimate users. This type of attack exploits vulnerabilities in cloud applications, web servers and databases.

5) **Insecure Interfaces, Application Programme Interfaces (APIs) and Virtual Machines (VMs):**

APIs are a set of standards and protocols than enable communication between different software applications via the internet. In the cloud context, APIs are implemented in the infrastructure, platform and software service levels in order to establish communications between various services. Cloud service providers generally provide their APIs to third party organizations in order to provide better services to their customers. Weak APIs can lead to the third-party organization acquiring the encryption keys and other important information about the cloud infrastructure. These encryption keys can be used to decode customer data and therefore compromise data confidentiality and integrity. Virtual machines and other software interfaces can be used by customers to gain access to the cloud infrastructure and services. These interfaces are generally used for management and monitoring of cloud activities. Exposure of these interfaces can lead to breaches in the access control, authentication and encryption policies. These attacks are usually a result of

poor key management mechanisms, Operating system bugs, bugs in the hypervisors and unpatched software (Aljumah & Ahanger 2020)

6) **Insider Attacks:**

Insider Attacks are usually internal to the cloud environment and is therefore harder to prevent and mitigate. These attacks are usually carried out by employees within the organization or business partners and third-party contractors who have access to the cloud infrastructure. Cloud Administrators are employees who have access to the organisations cloud environment which includes all the company's data and resources. Individuals may utilise these access privileges to leak company data for personal or other business purposes. The occurrence of these attacks can be reduced by conducting appropriate background checks before hiring employees, providing trainings to employees regarding security procedures followed within the organization and limiting access to company resources that are hosted on the cloud.

7) **Abuse of Cloud services:**

This type of threat usually occurs due to the misuse of cloud services by customers utilizing the cloud environment. These attacks are usually launched by hackers, spammers and other cyber-criminals in order to host malicious data, clog network resources, crack passwords and encryption keys and so forth. This threat usually has a higher impact on the cloud service provider than the service users (Kazim 2015). Lack of proper monitoring and establishment of appropriate service level agreements in the cloud environment usually results in these types of attacks. An example of this attack occurred in 2009 where attackers utilised the Amazons EC2 services as a control server that assisted in launching the Zeus botnet (Tirumala, Hira & Naidu 2015).

8) **Vulnerabilities with relation to shared technology:**

Cloud computing provides services where hardware and software resources are shared between multiple clients. The multi-tenant cloud infrastructure includes hypervisors that are utilised by customers to access their respective operating systems. However, these hypervisors have certain vulnerabilities associated with it which may result in hackers

acquiring inappropriate access to the Guest operating systems and therefore, the customer's data. This threat also occurs due to various shortcomings associated with Virtual Machines and third-party applications.

9) **Cloud Malware injection attacks (CMIAs):**

These attacks are usually launched with the intention to obtain access to the customer's data that is stored in the cloud. Structured Query Language (SQL) attacks and Cross-Site scripting attacks are two types of Cloud Malware injection attacks. These attacks usually take advantage of the vulnerabilities associated with the service providers cloud infrastructure.

The threats that were outlined in this section not only affect the cloud service providers but also have a huge impact on the enterprises that adopt the cloud computing technology. Therefore, it is important for cloud service providers and enterprises adopting the technology to understand the existing security policies and possible security threats in order to deploy a system with the right security policies implemented.

3. Related Works

The advancement in the modern cloud approaches undoubtedly is beneficial for users but it comes at the cost of increased security threats. The elasticity of the cloud environment involves front end and back end platforms with delivery models and network architecture. It is robust and more efficient than ever before but there are some challenging issues related to security which cannot be ignored. The researchers emphasize on making cloud security as one of the most important domains in the cloud environment. The study based on Cloud Security Alliance states that one of the biggest challenges in cloud computing is security and it is one of the reasons the enterprise sectors are reluctant to adopt cloud services.

According to Zissis & Lekkas (2012), the involvement of multiple parties/users in cloud increases the risk of data breach which in turn results as a threat to confidentiality. Multi-tenancy increases the risk of malicious attacks (Teneyuca 2011). Encryption/decryption is one solution for securing the transmitted messages. Kute et al. (2002) introduced two public key algorithms named RSA and ECC for generating random public key for the encryption and decryption process.

Kerberos authentication protocol is a ticket based secure protocol allowing nodes to communicate with each other securely in a non-secure environment by proving the identity. To manage and secure data in cloud, Hojabri & Rao (2013) implemented Kerberos authentication protocol.

Uma & Handa (2015) introduced a model for data security, using algorithms in storing and retrieval processes. The hiding algorithm was used for storing encrypted files behind images and the retrieval algorithm was used for separating the user data from the image. The proposed model involved client-side encryption and server-side steganography. To overcome the threat to sensitive data stored in cloud, Hyseni et al. (2018), suggested an increased confidentiality approach with various strategies for file encryption, partitioning and distribution among several storage providers. In the proposed methodology, prior to decryption, it would require looking for the parts of file saved in different storage platforms and then combine them, thus making it hard to decrypt the file.

Attar & Shahin (2018), proposed a model for concealment of information which comprised of two components with the primary part as uploading information and the secondary component as discharging information. The uploading information involved three phases where the first phase included data compression using WINRAR to occupy less space in cloud. In the second phase, a key was published with a strengthened forename and catchword for encrypting the information and saving securely in cloud using effective key management system. The last phase was to encode consumer information using AES encoding and storing in cloud. The secondary part called discharging information was data decryption using the derived key published by key administration system use AES method for decoding.

Sun et al (2018), addressed the security evaluation issues in cloud infrastructure and proposed a quantifiable security evaluation system for public, private, and mixed clouds using a coherent and reliable API. The evaluation was conducted using two cloud platforms sharing the network and was monitored using same security API. The evaluation model used a set of elements in cloud such as storage, network, application security etc, for calculating the total score to summarize the security view of architecture.

Singh & Saroj (2020), suggested a public auditing scheme to eliminate the data breaches by involving third party auditors for authenticating the privacy, reliability, and integrity of stored data. The proposed methodology consisted AES-256 algorithm for data encryption, SHA-15 for integrity checks and RSA-15360 for public key encryption. A research conducted by Morea &

Chaudhari (2016) proposed an approach where AES was used for data confidentiality, TPA (Third Party Auditing) for data auditing and SHA-2 used for generating message digest.

User authentication is a crucial parameter in cloud security. The researchers are constantly trying to develop a new strong methodology for user authentication to secure the cloud environment. For instance, Zhao et al. (2015) introduced an asynchronous challenge-response authentication solution involving hash function, symmetric algorithm, and combined secret key method as the components for user validation. To eliminate the possibility of guessing attacks the method generated random numbers, one-time secret key, and time-token, which in fact also avoided replay attacks .Vallabhu and Satyanarayana (2012), proposed a fused biometric authentication technique for single sign on to make service secure and reliable. Cryptography technique was used to store the biometric data and the registered user had to use the biometric authentication mechanism to access the services. Another approach suggested by Kumar, Kandavel & Madhavan (2020), introduced a multi-factor authentication technique where the validation procedure ends with a mystery key generation using AES cryptography calculation, client biometrics and secret word accreditations.

Arora et al. (2017) proposed Secure Cloud Ecosystem, catering the security for cloud from user authentication to data storage instead of conventional threat security systems. Multiple algorithms were used for better efficiency of the system in terms of security and reliability. The authentication process performed One Time Password (OTP), which was sent to the registered user email. Further, the salting technique called CSPRNG (Cryptographically Secure Pseudo-Random Number Generator) was used for password protection in case of password attacks in database. Also, to ensure password protection SHA_{512} and bcrypt hashing functions were used. The RSA public and private key generation is used along with the AES algorithm to encrypt the data. Dubey et al. (2012), developed a strong Java based authentication process for user identification in cloud architecture. The process begins with the user getting permission from the cloud for performing required operations and loading the data and ends with the cloud administrator asking for user permission to read and update the data. The model used RSA key generation for data encryption. The process involves 2 key generation from the client side. The client sends the first key appended with the message digest tag to the administrator, thus avoiding any alterations in key value (client) and tag value (Admin). Once the tag value is computed with the key value and authenticated, the administrator side updates the client. The client sends another key which is key 2 after approval from administrator side and then the final updating is done in the system. Finally, secure key 2 is saved in the log data and old keys are deleted for maintaining

consistency. MD5 hashing algorithm was used to generate message digest tag for providing digital identifier for each file.

The work presented by Islam et al (2019), suggests that one step authentication is not an effective approach to secure data and files in the cloud. Islam et al (2019), used cryptography and secure three step authentication process for cloud computing. The three-step authentication is a complex mechanism using two algorithms, one for the event when user logs into the system and one when user logs out of the system making it hard for attacker to break into the system. The process begins with the client logging into the system using registered userid and password. The system generates KEY1 using the stored KEY along with the hash function and sends it back to the user using a secured channel. The user enters the hashed KEY1 into the system again. The system uses anti-hash function on the KEY1 sent by the user thus decrypting it to KEY and further matches the KEY with the stored KEY. If matched successfully the system grants the access to the user. When the user logs out of the system, then the system generates a KEY2 along with hash function using KEY1. Further, the system encrypts the files and documents that has been accessed by the user using suitable encryption algorithm and then replaces KEY1 with KEY2 and exit.

Interesting researches were done on one of the important aspects of cloud security called searchable encryption. Han et al. (2016), stated that the searchable encryption is a scheme in which users access their encrypted data using secure search mechanism. Another work on secure search was presented by Xiang et al. (2016), where a new cloud database model was proposed. A database outsourcing protocol called SecureDBS was designed using secret sharing and tree-based order preserving mechanism. Hadavi et al. (2015), presented a multiple partitioning method for searching the data securely in a shared secret environment, thus preventing malicious inference attacks even if the attacker observes the data shares or queries. Fujinoki (2015), developed an attribute shuffling obfuscation mechanism where the degree of complexity was increased by increasing the number of obfuscated tables in database management system and increasing the network traffic load using the query constructor.

A study by Vaidya and Nehe (2015), suggested data slicing technique in cloud storage providing data security to the storage system in cloud. A middleware system is proposed for authenticating users for using the stored data at the backend storage with a layer of security. The middleware carried out file partitioning, splitting the file into multiple segments and saving them into backend cloud storage. Once the user sends a request to download the file, the system recreates the file and allows the download. Similarly, the concept of slicing was used by Subramanian and John (2018),

where an architectural framework for data sharing in the multi-cloud storage platform was proposed. The results from the work improved the security through dynamic slicing technique with the adoption of cryptography and encryption mechanisms. Another interesting proposal by Londhe et al. (2018), was a Division and replication strategy for storage security. The methodology involved fragmentation of the data and further replication and dispersion of the fragmented data so that the consecutive nodes do not hold the fragments of the same file. The usual approach of storing data in a single node was substituted with the data fragmentation and replication into strategic locations in the cloud to avoid data compromise due to single node exploitation.

Tysowski & Hasan (2013), proposed work where modified Attribute based authentication was implemented in a cloud computing environment. The purpose was to avoid the leakage of information during any network interception by the attacker. Negi et al. (2020), emphasized on the benefits of deploying Honeypot in cloud for intrusion detection and prevention. The conventional Honeypots are used as a bait against the attacker and provides all the relevant information of the intruder. The model proposed by Negi et al (2020)., suggested the implementation of Honeypot by using an application, which is not limited to providing attacker information but also providing security to the cloud infrastructure. In cloud, millions of users are part of same physical infrastructure sharing same data centres, thus, increasing network security risk. Chen et al. (2014), suggested a collaborative prototype system for network security in multi-tenant data centre. An open source UTM system was implemented where level-based packet inspection and security plugins were installed according to the level-based protection policy.

4. Reflection

This section of the report will critically analyse the approaches to mitigate cloud security threats that were discussed in section 3 of this report.

Uma & Handa (2015) suggested a method for providing data encryption during the transmission of data between the client and the storage devices and while its stored on the sever-side. The proposed methodology utilises AES algorithm to provide client-side encryption of data. The encrypted data is then transmitted to the storage device. The storage device utilises a hiding algorithm to store the encrypted data behind images. This process of concealing data utilising images is called steganography. Although this procedure provides two-level encryption of client data, it contains certain drawbacks. This approach does not provide mutual authentication between the clients and servers. Therefore, in case the identity of the client or server is compromised, the

other party would not be able to identify the potential attack and will continue communications. Another drawback with this approach is in case the client-side encryption keys are compromised, the attacker will be able to decrypt the client data while its being transmitted to the specific server. The utilization of steganography to provide encryption of data on the server-side also has some potential drawbacks. There are specialised software's in the market that can easily decode steganographic images to extract the relevant data. Uma and Handa(2015), in their journal publication, failed to describe the potential benefits of utilising steganography with images over other methods to provide encryption-at-rest for client data.Therefore,the security model proposed in the journal publication addresses certain key security-related issues but fails to illustrate the advantages of the proposed model and take in to account key security-related features such as Mutual authentication between the communicating parties.

However, the security model proposed by Uma and Handa (2015), can be enhanced by utilising the file partition methodology described by Hyseni et al. (2018). The file partitioning method that is proposed involves partitioning the encrypted client data into smaller chunks and storing each of these chunks in different storage servers.Therefore,in case an attacker wants to obtain access to the client data, the attacker must locate the source of the different parts of the data, combine the parts and then attempt to decrypt the data. This approach of storing the various portions of client data in different servers can be used in conjunction with the encryption utilising steganography with images that was suggested by Uma and Handa (2015).This can be achieved by partitioning the encrypted client data and encoding it behind different images using steganography on multiple servers rather than encoding the entire data behind a single image on an individual server. However, the drawback with the approach suggested by Hyseni et al. (2018) is that the file partitioning algorithm works only for specific types of files with considerably lower file sizes. The maximum file size tested on the model was 2969KB. The proposed model does not promise similar results with larger file sizes and different file formats. Another drawback of the file partitioning algorithm proposed is that the algorithm does not describe the basis on which the various portions of the file are divided between the multiple storage nodes. In order to improve security and ensure the attacker doesn't easily track the location of the fragmented client data, it is important that the servers elected to store the fragmented data are not adjacent to each other and have a significant geographical distance between them.

The issue of fragmented data being located on adjacent nodes is resolved by an approach suggested by Londhe et al. (2018). This approach provides a mechanism for fragmenting the client data, ensuring the fragmented data is not stored on adjacent nodes in the cloud infrastructure and

replication of the fragmented data, thus ensuring availability of data even if a single node is down. The T-Coloring algorithm is utilised to ensure that fragmented data is not stored in adjacent nodes. The T-Coloring algorithm is used to first identify the nodes that will store the original fragments of the client data and then the nodes that will store the replicated fragments.Although,the approach suggested in this paper solves the issue of fragmentation and replication of client data ,it doesn't describe the security of the fragments at the server nodes.

Singh and Saroj(2020) described an approach for encryption of client data (during transit and when it is stored on the storage device) and performing audits on the client data in order to ensure integrity of the stored data. The proposed methodology suggests utilising AES-256 algorithm for data encryption, SHA-15 for integrity checks and RSA-15360 for public key encryption. Morea et al. (2016) proposed an approach utilising AES for data confidentiality, TPA (Third Party Auditing) for data auditing and SHA-2 for generating the message digest. The approaches described in these two papers ensure the confidentiality and integrity of client data utilising strong encryption mechanisms and integrity checks. However, the approaches suggested in these papers do not ensure mutual authentication between clients and servers in the cloud environment. This drawback could lead to attackers utilizing rogue client devices to gain access to the cloud environment and launch Denial of service attacks hampering availability of cloud services to legitimate clients. Another drawback of the approaches suggested in these two papers is the utilisation of third-party auditors to ensure data integrity. As suggested by Razaque & Rizvi (2017), the utilisation of third-party auditors for performing integrity checks can itself introduce additional security vulnerabilities to client data.

Zhao et al (2015) in their publication "Asynchronous Challenge-Response Authentication Solution Based on Smart Card in Cloud Environment" proposed a methodology for achieving mutual authentication between the client and the cloud infrastructure. This method introduced an asynchronous challenge-response authentication solution involving hash function, symmetric algorithm, and combined secret key method as the components for user validation. The method also eliminated the possibilities of guessing and replay attacks by utilising random numbers, one-time secret keys, and time-tokens. However, the utilisation of hash functions to secure user credentials has certain drawbacks. Brute-force algorithms can be used to extract the original passwords from the hashed functions and hence compromising customer data. Another drawback with the proposed methodology is that in case an attacker manages to gain access to a particular cloud server; they also gain access to the combined secret keys which is stored on the server itself.

Obtaining access to the combined secret keys stored on the server may lead to the exposure of customers data.

Vallabhu and Satyanarayana(2012), suggested an approach to achieve mutual authentication between clients and servers utilizing biometric systems embedded in the cloud infrastructure. Biometric systems can be used to identify users based on physiological and behavioural attributes. The method suggested in this paper utilises a blind protocol technique in order to ensure that the biometric information collected is not utilised for extracting any other information about the user or about the biometric to the server authenticating the user and vice-versa. The blind protocol technique also provides encryption capabilities to the biometric data that is collected. The approach suggested in this paper which Utilises biometrics to identify and validate users contains certain drawbacks. Although the blind protocol technique provides encryption of the biometric data on the server-side, encryption of the biometric credentials during transit is not addressed. The paper also does not describe the type of encryption algorithm that is used to secure biometric information. Leakage of biometric data could pose as a serious threat to the privacy of individual users. Another drawback of utilising biometrics for mutual authentication is that the large amount of biometric information in the cloud environment could lead to computational complexities, thereby, leading to a reduction in the speed of responses from authentication servers (Albahdal & Boult 2014). This drawback could lead to vulnerabilities such as the Man-in-the-middle attack. Another potential drawback of utilising biometrics to identify users, is the possibility of inaccuracies in the biometric calculations which could lead to authentication inefficiencies.

Islam et al. (2019) proposed a three-step solution for achieving mutual authentication between clients and servers in the cloud environment. The proposed solution consists of the following steps:

1) A user logs in with their Username and password.
2) In case the credentials provided by the user are valid, the server generates KEY1 using the stored key associated with that user and a hash function.KEY1 is then sent to the user via a secure channel such as an email or a text message.
3) User receives KEY1 and sends it back to the server. The server checks the validity of the KEY1 sent by the user and uses an anti-hash function on KEY1 in order to retrieve the original key.
4) The server then compares the key retrieved from the anti-hash function and the stored key associated with the user. In case, all the information exchange between the user and server is valid, the user is granted access to the system.

The proposed system also provides a methodology for encrypting the data stored by the user once the user logs out of the server. Once a user logs out successfully, the server generates a second key KEY2 using a hash function on previously used KEY1.The data stored in the cloud server is encrypted using KEY2.

The solution provided for mutual authentication and encryption of client data ensures that even if an attacker acquires user credentials ,the attacker will still not be authenticated by the server as the attacker wont have access to KEY1 which is supplied only to valid users. The proposed system also provides protection to the data stored in the cloud environment against potential attacks by ensuring all stored data is encrypted. The drawback with the approach suggested in this paper is that there is no encryption procedure specified for the exchange of user credentials and data between the client and the associated cloud servers. The paper also does not describe any particular encryption algorithm that is utilised for encrypting client data.

Negi et al (2020) proposed a solution to provide security to the cloud infrastructure utilising Honeypots. Honeypot is a system which can be utilised to imitate probable targets of potential attackers. They can be used to detect potential attacks, deflect these attacks away from the actual cloud environment to the Honeypot framework and extract valuable information about the attackers. Honeypots in the cloud environment can be used to identify potential attacks to the cloud infrastructure as well targeted attacks on their customers. As suggested by Negi et AL, Honeypots can be implemented as a physical device in the cloud data centres or as an application deployed on a server in the cloud.

5. Research Proposal

The reflection section of the report critically analysed the existing approaches utilised to secure the cloud environment. From the performed analysis, the following inferences were drawn:

1) Although certain approaches suggested strong encryption mechanisms for data-at-transit and data-at-rest on the cloud servers, the mutual authentication functionality was not addressed.
2) There were certain approaches that suggested mechanisms for mutual authentication between the clients and servers. However, these approaches failed to define encryption mechanisms for the client data while at transit and while being stored on the cloud servers.

This section of the report addresses these drawbacks by proposing a cloud security framework which addresses the following functionalities:

- Mutual Authentication between the clients and the cloud infrastructure.
- Encryption of data during transmission between the client and the cloud servers
- Encryption of data when stored on the cloud servers
- Fragmentation and replication of client data.
- Deployment of Honeypot for securing the cloud servers

1) Mutual authentication between the clients and the cloud infrastructure:

The proposed security framework will utilise the authentication mechanism described by Islam et al. in conjunction with encryption mechanisms such as Advanced encryption standard (AES) and Rivest–Shamir–Adleman (RSA) in order to provide mutual authentication between clients and the cloud servers. The procedure for mutual authentication between clients and servers is as follows:

1. A user logs in with their ID and password. This information is encrypted using RSA algorithm and sent to the server for verification.
2. The server on receiving the encrypted information, extracts the user credentials and confirms its validity. In case the user credentials provided is valid, the server generates KEY1 using the stored key associated with that user and a hash function.KEY1 is then sent to the user via a secure channel such as email or a text message.KEY1 is encrypted using AES Algorithm while it is transmitted to the user.
3. User on receiving KEY1 from the server, encrypts it using AES algorithm and sends it back to the server.The server checks the validity of the KEY1 sent by the user and uses an anti-hash function on KEY1 in order to retrieve the original key.
4. The server then compares the key retrieved from the anti-hash function and the stored key associated with the user. In case, all the information exchange between the user and server is valid, the user is granted access to the system.

RSA encrypted messages utilise public keys which can be shared in public. However, these public keys can only be decrypted using private keys. On the other hand, AES is a symmetric algorithm utilising a single shared secret key which is used to encrypt and decrypt messages.RSA is excellent for key exchange but is slower than AES.However,AES is much faster but suffers from security-related risks as a single key is used for both encryption and decryption. The security framework

proposed in this report utilises the advantages offered by RSA for the initial exchange of credentials and utilises the speed and efficiency of AES for all further communications between the client and server.

2) Encryption of data during transmission between the client and the cloud servers

The framework proposed in this report will achieve encryption-in-transit functionalities utilising 128-bit AES SSL/TLS encryption.

3) Encryption of data when stored on the cloud servers

The encryption of data-at-rest will be achieved using 256-bit AES encryption.

4) Fragmentation and replication of client data.

The proposed framework will utilise the file partitioning and replication mechanism as explained by Alka et al in their conference publication. This mechanism will ensure the client data that arrives in the cloud infrastructure is first fragmented and stored in multiple servers. This fragmented data is then replicated and again stored in multiple servers. The framework also utilises T-Coloring algorithm to ensure that the fragmented and replicated data is not stored on adjacent storage devices in the cloud.

5) Deployment of Honeypot for securing the cloud servers

The framework proposed in the report will utilise Honeypot as an application on the cloud databases to prevent malicious attacks on the cloud environment. The deployment of honeypot in the security framework will enable cloud service providers to deflect potential attackers from the actual cloud infrastructure and extract information about the attacker. Honeypots can also provide information about the intent of the attacker and the systems the attacker is attempting to target.

6. Conclusion

The proposed security framework suggests high security mechanisms taking various possible breaches into the consideration. The suggested model is reliable and fast. The framework covers the authentication procedure with highly secure three step mechanism using combination of RSA and AES encryptions. Further, file partitioning and replication technique is used for data storage and finally honeypot system is deployed as a decoy for malicious attacker to avoid database attacks such as SQL injection. It conforms with the CIA (Confidentiality, Integrity, Availability) triad, a security model.

7. References

- Albahdal,A.A. & Boult,T.E. 2014, "Problems and Promises of Using the Cloud and Biometrics," 2014 11th International Conference on Information Technology: New Generations, Las Vegas, NV, pp. 293-300.
- Aljumah, A., Ahanger,T.A.,2020, "Cyber security threats, challenges and defence mechanisms in cloud computing," IET Communications, vol. 14, no. 7, pp. 1185-1190
- Arora A., Khanna A., Rastogi A. & Agarwal A. 2017, "Cloud security ecosystem for data security and privacy",*7th International Conference on Cloud Computing, Data Science & Engineering - Confluence*, Noida, pp. 288-292.
- Attar, N. & Shahin,M. 2018, "A Proposed Architecture for Data Security in Cloud Storage Space", *Journal of Biostat and Biometric Application*, 201.
- Caroll,M., Merwe,D.V.A. & Kotzé,P. 2011, "Secure cloud computing: Benefits, risks and controls," *2011 Information Security for South Africa*, Johannesburg, pp. 1-9.
- Chen,Z.,Dong,W.,Li,H.,Zhang,P.,Chen,X. & Cao,J. 2014, "Collaborative network security in multi-tenant data center for cloud computing," in *Tsinghua Science and Technology*, vol. 19, no. 1, pp. 82-94".
- Columbus, L.,2018," State Of Enterprise Cloud Computing, 2018",Forbes,30 August,< https://www.forbes.com/sites/louiscolumbus/2018/08/30/state-of-enterprise-cloud-computing-2018/#2e378345265e>
- Dubey, K.A.,Dubey, K.A., Namdev, M. & Shrivastava, S.S. 2012, "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", *Software Engineering(CONSEG) CSI Sixth International Conference*, pp. 154-159.
- Fei,H., Jing,Q. & Jiankun,H. 2016 " Secure searches in the cloud: A survey" Future Generation Computer Systems. 62. 10.1016/j.future.2016.01.007.
- Hiroshi, F. 2015, "Designs, analyses, and optimizations for attribute-shuffling Obfuscation to protect information from malicious cloud administrators", Security and Communication Networks 8(17):3045–3066
- Londhe,A., Bhalearao,V., Ghodey,S., Kate,S., Dandekar, N. & Bhange, S. 2018, "Data Division and Replication Approach for Improving Security and Availability of Cloud Storage", *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, Pune, India,pp.1-4.
- Mohammad,H., Rasool, J., Ernesto,D. & Stelvio, C. 2015, "Security and searchability in secret sharing-based data outsourcing", International Journal of Information Security. 14. 10.1007/s10207-015-0277-x.
- Subramanian,K. & John,L,F. 2018, "Dynamic and secure unstructured data sharing in multi-cloud storage using the hybrid crypto-system", International Journal of ADVANCED AND APPLIED SCIENCES, vol. 5, pp. 15.

- Gao, G,S., Ji, T. & Tu,X. 2018,"One Quantifiable Security Evaluation Model for Cloud Computing Platform", *2018 Sixth International Conference on Advanced Cloud and Big Data (CBD)*, Lanzhou, pp. 197-201.

- Handa, K. & Uma,S.S. 2015, "Data Security in Cloud Computing using Encryption and Steganography", *International Journal of Computer Science and Mobile Computing*, vol. 4, no. 5, pp. 786-791.

- Hojabri.M. & Rao.V.K. 2013, "Innovation in Cloud Computing: Implementation of Kerberos version5 in cloud computing in order to enhance the security issues" IEEE, International Conference onInformation Communication and Embedded System(ICICES), pp 34-45.

- Hyseni, D., Selimi, B., Luma, A. & Cico, B. 2018, "The Proposed Model to Increase Security of Sensitive Data in Cloud Computing", *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*, vol. 9, no. 2, pp. 203-210

- Islam,J.M.S, Chaudhury, H.Z. & Islam,S. 2019, "A Simple and Secured Cryptography System of Cloud Computing", Electrical and Computer Engineering (CCECE) 2019 IEEE Canadian Conference of, pp. 1-3

- Kazim,M.,Zhu,Y.S.,2015," A survey on top security threats in cloud computing", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 3,pp. 109-113

- Kleyman,B.,2015," Security Breaches, Data Loss, Outages: The Bad Side of Cloud", Data Centre Knowledge, March 16,https://www.datacenterknowledge.com/archives/2015/03/16/security-breaches-data-loss-outages-the-bad-side-of-cloud

- Kumar, S.G., Kandavel, N. & Madhavan, K. 2020, "To Discovery The Cloud Services Authentication An Expert Based System Using Multi-Factor Authentication", *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, pp. 1014-1016.

- Kute B, Vivek.R ,Paradhi.P. & Bamnote G. 2002, "A SOFTWARE COMPARISON OF RSA AND ECC", *International Journal Of Computer Science And Applications*, pp. 2.

- Morea,S. & Chaudhari,S. 2016, "Third Party Public Auditing Scheme for Cloud Storage", *International Journal of Prpcedia Computer Science*, vol. 79, pp. 69-76.

- Negi, S.P., Garg,A. & Lal,R. 2020, "Intrusion Detection and Prevention using Honeypot Network for Cloud Security," *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, pp. 129-132.

- Pedigo,C.,2019," The Biggest Cloud Breaches of 2019 and How to Avoid them for 2020",Lacework,December 13,< https://www.lacework.com/top-cloud-breaches-2019/>

- Razaque, A. & Rizvi, S.S. 2017, "Privacy preserving model: a new scheme for auditing cloud stakeholders.", J Cloud Comp 6, 7.

- Reddy, T,G., Sudheer,K., Rajesh,K. & Lakshmanna, K. 2015,"Emplolying Data Mining on Highly Secured Private Clouds for Implementing a Security – as a – Service Framework", *Journal of Theoritical and Applied Information Technology*, vol. 59, no. 2.

- Singh,P. & Saroj,K.S. 2020, "A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage," *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, pp. 695-700.

- Teneyuca.D. 2011, "Internet Cloud security: the illusion of inclusion", *SciVerse ScienceDirect*.

- Tysowski,K.P. & Hasan, A.M, 2013, "Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds," in *IEEE Transactions on Cloud Computing*, vol. 1, no. 2, pp. 172-186.

- Tirumala,S., Hira,S. Naidu, V., 2015," Analysis and Prevention of Account Hijacking based Incidents in Cloud Environment", 14th International Conference on Information Technology, ICIT-2015,India

- Unbound,2016," Secret Key Vulnerabilities: Think You're More Secure than Instagram?",< https://www.unboundtech.com/secret-key-vulnerabilities-think-youre-more-secure-than-instagram/

- Vallabhu, H. & Satyanarayana,V.R. 2012, "Biometric Authentication as a Service on Cloud: Novel Solution", *International Journal of Soft Computing and Engineering (USCE)*, vol. 2, no. 4, pp. 163-165, September 2012, ISSN 2231–2307.

- Vaidya, B.M. & Nehe,S. 2015, "Data security using data slicing over storage clouds," *2015 International Conference on Information Processing (ICIP)*, Pune, pp. 322-325.

- Xiang,T., Li X., Chen F., Guo S. & Yang,Y. 2016, "Processing secure, verifiable and efficient SQL over outsourced database", Inf Sci 348, 163–178.

- Zhao, G., Li,L., Du,L. & Zhao,X. 2015, "Asynchronous Challenge-Response Authentication Solution Based on Smart Card in Cloud Environment", *2015 2nd International Conference on Information Science and Control Engineering*, Shanghai, pp. 156-159.

- Zissis, D. & Lekkas, D . 2012, "Addressing cloud computing security issues." Future Generation Comp .Syst.28. 583-592. 10.1016/j.future.2010.12.006.

- *Singh.P & Saroj.K.S. 2020, "A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage,"* 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India,pp. 695-700.*