Comput Syst Sci & Eng (2020) 5: 357–366


International Journal of
Computer Systems
Science & Engineering

# Secure Information Access Strategy for a Virtual Data Centre

**Sivaranjani Balakrishnan**[1]* **and Dr. D. Surendran**[2]†

[1] *Department of Computer Science and Engineering, Government College of Engineering, Bodinayakkanur, Theni Dist, Tamilnadu, India*
[2] *Professor, Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore - 641 407, Tamilnadu, India*

With the arrival of on-demand computing, data centre requirements are extensive, with fluid boundaries. Loaded Internet applications, service-oriented architectures, virtualization and security provisioning are the major operations of a data centre. Security is an absolute necessity of any network architecture, and the virtual IT data centre is no exception. At the boundary, security is focused on securing the terminals of the data centre from external threats and providing a secure gateway to the Internet. The paradigm shift towards a new computing environment makes communications more complicated for Infrastructure Providers (InP). This complexity includes the security of the data centre's components to protect data from malicious attacks or from being compromised. Threats/attacks are inevitable if the data are generated from a public network, such as Wi-Fi in an Airport, Railway station and other public places. Since these places create enormous amounts of data from anonymous and naive users, it is essential to store the information in a data centre. In this article, we propose an efficient, secure, and privacy-preservation information access algorithm to access data centres in public wifi networks. This algorithm is based on the primitive root approach for sending and receiving credentials through the anonymous authentication of the users and ensuring protected data access from the data centre. Security and Performance Analysis and its evaluation prove that our approach is successful with respect to security, privacy preservation and computational complexity.

Keywords: Virtual data centre, Data centre Security, Primitive root, Dummy parameters, Pseudo parameters, secret key, public key, Customer Master Key

## 1. INTRODUCTION

### 1.1 Cloud Data Centre

Infrastructure as a service(IaaS) is the ability to create, manage and consume infrastructure elements such as OS images, storage volumes, and network and computing resources. Data centres have become a vital part of information storage and retrieval through high end communication channels. Data centre components are the main building blocks of cloud computing. These components basically include various redundant components, such as computing and networking components, power supplies, data communication channels and environmental control and security devices, to provide uninterrupted consumer service. Companies were migrated from Internet Data Centres (IDCs) to Cloud Data Centres (CDCs) for easier deployment and operations. To load the information into the data centre, different types of storage methods have to be used. The stored information in the data centre is classified based on its usage and origin. This classification enables the end users to load their information to be retrieved later. Data centres do have different physical servers and storage elements for the users. These data centres are vulnerable to security attacks since they hold sensitive information, such as banking information, personal information, and so on.

### 1.2 Virtual Data Centre (VDC)

Corporations, governments and social media are moving faster towards community data centres to achieve uniform and secure data storage. Data centres have been transformed into Virtual Data Centres in the recent years due to virtualization technology. Virtual data centres have quickly emerged in computing environments due to their vast benefits such as faster redeployment, better data centre resource utilization, reduced costs, easier backups, greener pastures, less vendor lock-in, better disaster recovery, single minded servers, etc.

*Email: bsranjani@gmail.com
†Email: d.surendran@gmail.com

Virtualization of data centre components tends to lower capital and operational expenses and reduce energy consumption and supports providing services based on a subscription basis. In virtual data centres, resources are shared among multiple tenants. The servers and storage could be concurrently used for different VDC end users to achieve efficient resource utilization. A VDC is basically a multi-tenant environment, and provisioning security for the stored data becomes mandatory.

## 1.3 Threats to Data Centres

Due to the multi-tenant nature of virtual data centres, they are prone to security breaches based on the essence of the stored information. Due to the evolution of cloud computing, the data centre operations have become more virtualized, dynamic and service oriented with fluid boundaries. The security policy for each client may vary according to their needs and the type of data storage [1].

Over the years, the annual expenditures towards cloud security have increased by 10%. These costs impact the trustworthiness of cloud customers who are loading the sensitive data. Evaluation metrics of cloud security services have been proposed to assess the services' security.

Data centre security breaches include three categories such as threats, vulnerabilities and attacks. The most common threat for data centres could be DoS (Denial of Service) attacks, leaks of confidential information, data theft or alteration, the unauthorized use of data centre resources and identity theft. Threats can occur during transmission or at the time of storage.

Web browsers are the main offenders in leaking the information from standalone systems [28]. Public clouds and community clouds are more vulnerable to security attacks than private clouds since they share their virtualized components with others [11].

DoS attacks degrade the services that are provided to the legitimate users when performing their regular activities in the data centre. Network Protocols, such as TCP and ICMP in the network infrastructure, are vulnerable to this attack. In distributed DoS attacks, a large number of resources are compromised due to the scattered resources and the lack of coordination. These attacks target the servers rather than the data centre network infrastructures. The internet is a vital part of cloud since all the services are accessed through the internet from the data centre. Internet infrastructure attacks crash the entire network instead of individual systems and servers.

Trust Exploitation is a data centre attack that exploits the trust between the communication resources in the data centre. The web server in a data centre ought to trust a backend database to retrieve the data. Session hijacking activity steals legitimate sessions between the target data centre and trusted hosts to deny the communication. Buffer overflow attacks occupy more space in the memory than is actually reserved for it.

Amazon CloudFront accelerates the distribution of the static and dynamic content of web pages with the lowest latency. For this purpose, it places the content in edge locations to deliver the contents without any delay. The content is not secured as promised by the cloud providers in terms of the location of the stored content and the physical server is shared among other local tenants [3].

It is the responsibility of a cloud service provider to ensure security in terms of Availability, authenticity, access control, integrity and confidentiality to guarantee secure end-to-end communications [10]. Security is proposed for various points, such as the network, virtualization, web applications and the physical equipment, in the cloud environment [24]. To protect the VDC resources from potential threats and to assure authentication, information confidentiality and integrity, users have specific security demands and requirements.

Remote access is another reason why security enforcement is vital in a data centre. Cloud Operators/Service providers often require remote access to the data centre to perform new service activations or maintenance. This remote access must be properly secured and accurately monitored to ensure that only authorized users are always permitted to access the data centre resources. Robust authentication, authorization and accounting strategies should be integral to ensure that only authorized users are allowed to access the datacentre.

Pseudo identity-based authentication has evolved to help mobile entities communicate without revealing their real identities. However, its computation costs grow linearly with the communication load. The public-private key pair should be updated each time when the node pseudonym is changed, and thus the computational overhead increases linearly with the number of applied pseudonyms. The proposed scheme uses un-linkable pseudo-IDs of the Network users.

In this paper, we consider the security for virtual data centres as mandatory. Firstly, providing authentication for any secure transmission is the first defence against any security attack in a virtual data centre. Authentication is the process of verifying the user's credentials in a secure and efficient way. These user credentials may be an email id, mobile number, SSN, etc. All these credentials are called the user's real identities. However, during authentication, it is not compulsory to authenticate the users using their real identities. Instead of using real identities, a pseudo identity for user authentication is presented between the end user and the VDC resource. By using these Dummy identities, the user's privacy is always protected in an anonymous manner. Mutual anonymity is required to shield the sensitive data from malicious users. Moreover, the authentication process provides an inference that only the authenticated users can perform communications instead of malicious users. The merits of anonymous logins include convenience, ease of use and free public information.

Secondly, the Data integrity includes maintaining the consistency, accuracy and trustworthiness of the data over its entire life cycle of data transmission. Preserving data integrity is a core focus of our paper. The proposed algorithm prevents data from becoming lost, garbled or modified without the end parties' consent. This algorithm works in addition to traditional security mechanisms, such as firewalls, antivirus filters and intrusion detection systems.

In summary, we are proposing a scheme for VDC data security verification. The added benefit of this is that it cuts the communication overhead and increases the efficiency of the security verification process for Data centres. Our proposed scheme is competent in comparison to Prime number-based algorithms since it reduces the computational load and execution time significantly; furthermore, it also strengthens the security of the data, which is the main focus of this paper. The research work of the paper can be summarized as follows.

- We present a secure VDC communication architecture.
- We design and develop an efficient Primitive Root Based Secure Information Access algorithm for Data centres.
- We evaluate our proposed algorithm using simulations and show that our solution is efficient when applied to conventional VDCs in comparison to Prime number-based techniques.

The performance analysis of our scheme shows that the proposed method has better performance than existing authentication schemes in wireless communications in terms of security, privacy, and efficiency. Based on this scheme, both user privacy and trustworthy public Wi-Fi networking can be achieved. The paradoxical notion of anonymous authentication is performed without revealing users' identities.

The structure of this paper is organized as follows. Section II describes the various research works related to cloud security challenges and overcoming the security threats and vulnerabilities in data centres. Section III elaborates the proposed system architecture with its relevant model. In section IV, our algorithm is explained and the proof of the algorithm is provided. In section V, the security analysis and performance evaluation of the proposed algorithm is shown. Section VI concludes our paper with future possible research directions.

## 2. RELATED WORK

In this section, we have summarized the related works that were carried out to improve the security of virtual data centres. Very few works were conducted in previous years related to providing security in VDCs. Nevertheless, most of the existing schemes failed to satisfy the security requirements of VDCs due to their specific characteristics. Meanwhile, a negative correlation between privacy and security yields an additional challenge: more privacy means that it is harder to achieve non-repudiation and accountability.

Various surveys have been conducted on cloud security based on vulnerabilities, attacks, threats, its adoption and its challenges. These surveys monitor the performance impact after the successful security provisioning. This survey overlooked various security challenges and the possible solutions to enhance the security in the multilayer cloud environment. A three-layer security was proposed for the application, middleware and infrastructure layers [11,19,26,27]. For multiple cloud environments, application level security had been applied through user access control. This approach preserves the user's private space and application level security from multiple vendors [20].

M.A.Khan had particularised the attacks and security issues in the cloud environment. Attacks are grouped based on networks, VMs, storage and applications. This categorization proactively eases the avoidance and prevention of attacks [18]. According to various reviews and studies, it is well noticed that cloud security needs more insights on privacy, non-repudiation, recovery and prosecution [22].

The embedding of virtual links and nodes in the physical counterparts causes security breaches in data centre networks. S. Berger et al. [2] implemented the isolation among VDCs to reduce the mapping time. The authors also guaranteed the integrity among virtualized resources. Many technical surveys used various metrics to employ security at all levels. Further heuristic algorithms were developed to address the virtual network embedding problem and to provide security for virtual resources [12, 13, 14, 16 and 33].

Cong Wang et al. proposed a scheme to securely store cloud data and retrieve the data without any modification. Since cloud data are dynamic in nature, they proposed error correcting methodologies [4]. In [5], the authors designed an auditing system for the distributed and autonomous agent model to generate the set of rules for the current situation to extract the security events. Multi-layered security was provided to proactively store data around firewalls, identity management and encryption [7]. However, this Adoption Framework fails to preserve the privacy of the sender and the receiver. Conventional firewalls work based on the predefined policies and rules, but they fail to react to unauthorised access through malicious code injections into the network [8].

Cloud data can be secured using traditional cryptographic methods such as Public Key Cryptography. Dimitrios Zissis et al. proposed a scheme that used trusted third-party certificates to ensure authentication, integrity and confidentiality [6]. A DMZ (demilitarized zone) is created in the datacentre to provide an additional security layer to the resources in a Cooperative Virtual Data Centre (CVDC). Two firewalls are employed to provide protection from threats from the internet and the local network [9].

A self-Cleansing Intrusion Tolerance system was developed by Iman EL MIR et al. for a single Virtual machine in a data centre [12]. This analytical model requires more time to cleanse the Intrusion from the data centre.

PaaS layer security is provided for the service instances that threaten other users [15]. Security ought to be provided to the upper layers of services, such as SaaS, PaaS and IaaS. Since attacks cause major problems such as network traffic, inconsistent data storage and server crashes, it is mandatory to protect the data centres at the physical level.

Data labels for the incoming data are provided for all the data blocks. This approach categorizes the type of data to provide security. A transparent encryption method is also proposed through a trusted device [21]. A Role Based Access Control (RBAC) Mechanism is suggested for the protection of information in the data centre. All the virtual resources are assigned role-based access controls to control data leakage vulnerabilities [15, 23, 25]. The number of roles increases to properly provide permissions within the data centre. Thus, RBAC suffers from role explosion. Managing all the roles can become a complex affair for the Service Provider.

A Cloud Computing Adoption Framework has been proposed to provide extra layers of security in the simulation through the Business Process Modelling Notation (BPMN). This framework will eventually increase the overhead of the data centre and the latency of the data storage [7, 30].

The access time of data from data centres increases when the layers of security are strengthened. S. Namasudra et al proposed a secure DNA based access control model for cloud environments, which focuses on reducing the search time, access time and overhead by using different encryption keys for the same data [29].

Yibin Li et al proposed architecture for splitting the sensitive data and normal data from the cloud users using the Alternative Data Distribution (AD2) Algorithm and the Secure Efficient Data Distributions (SED2) Algorithm. The process of retrieving data from data centres is accomplished using the Efficient Data Conflation (EDCon) Algorithm [31]. The splitting process adds more overhead to the orchestration tool.

A Dynamic Prime Number based efficient security mechanism for data streams has been proposed and provides security using symmetric cryptography and random prime number generation. The key is initialized dynamically to support real time protection against threats and to reduce the latency that is created due to enhanced security [34].

Bruno et al. clearly decreased the overhead that was created by providing enhanced security to data centres. These overheads will assuredly affect the QoS parameters and the SLA between the provider and users [32]. In paper [17], the authors identified an issue that leads to vendor lock-in for customers. Since the security provisioning of the data centre leads to Data lock-in with the cloud provider, this issue significantly disturbs the security mechanism that is provided to the end users' information that had been stored in the vendor's proprietary format.

Traditional privacy enhancement techniques usually apply node pseudonyms in public networking to conceal real identities and avoid privacy tracking.

To achieve a high utilization rate and green computing, virtual machines are often migrated between physical servers. During server consolidation, virtual machine movement is mandatory to reduce the energy consumption, which makes data centres susceptible to security breakdowns. Due to the movement of VMs, the cloud environment is highly prone to security attacks. It is also inevitable that multiple tenant VMs may stay in a single physical server, which leads to security threats for the tenant data.

In summary, virtual data centres are prone to security breaches since they host the data of multiple tenants in the same physical server. Due to the storage of sensitive data in the cloud, it is mandatory to provide high security for the VDC, including storage and transactions. The methods and algorithms proposed in this paper were centred on the security provisioning based on the pseudo identities of the customers to prevent identity theft and unauthorized data access. In this paper, we propose a security scheme that works based on the primitive root that is used in ElGamal Cryptosystems. This algorithm ensures the preservation of the real identities of the end users and prevents unauthorized data access.

# 3. PROPOSED SCHEME

## 3.1 System Architecture

In this section, we first study VDC embedding and associated security issues in virtualized data centre environments. Before proceeding with the algorithm, the prerequisites were also discussed. A brief discussion of the system model for running the Secure Anonymous authentication Algorithm is presented. Then, the rationale for enforcing the proposed security scheme during the process of virtual data centre request embedding is discussed.

### 3.1.1 VDC Embedding

VDC Embedding is performed in two phases as shown in Figure 1. Firstly, the virtual resources (VMs, virtual switches and routers) in the request are mapped to the physical data centre by assigning the server instances and core/aggregation/Top of Rack switches. Secondly, the virtual links between the assigned virtual resources are embedded. This embedding process is carried out by protecting the performance of the entire VDC in terms of the agreements made through the SLA between the Infrastructure Provider (InP) and the Service Provider (SP).

The guaranteed performance of the VDC must be delivered to the end customer to maintain the credibility of the InP and SP. The promised QoS parameters, such as High availability and intra and inter Bandwidth for communications, and the configuration of the VMs are to be assured. By keeping these parameters intact, the security of VDCs is reinforced.

### 3.1.2 Security Issues in Virtual Data Centre Embedding

Since a VDC is basically a multitenant data centre, it is vulnerable to security attacks. All the customer resources reside in the data centre as a VDC, including the localized network infrastructure. The VMs can be affected by the collocated VMs that are under security threats since they share the same physical server. Similarly, the substrate networks are shared by the VMs and are allocated by different VDC requests through virtual switches and virtual links. Hence, it is inevitable that defence must be provided against all the attacks and threats that happen inside and outside of the data centre. Multifactor authentication is mandatory in a data centre when the entire data centre is virtualized.

### 3.1.3 Prerequisites of Security Provisioning

There are certain secure schemes that need to be applied at the time of embedding the VDC requests into the physical Data Centre to ease the workloads of security algorithms and during the server consolidation phase.

The security preliminaries that are to be followed are as follows.

i. Assign the VMs that belong to same VDC request into the same physical server as much as possible to isolate the requests.

ii. Enforce user side data encryption/ decryption for better data confidentiality.

iii. Apply Role Based Access Control (RBAC) to limit the resource access based on the authentication.

## 3.2 System Model

As a support to the general security model shown in Figure 2, we developed an optimal security model. The model consists of three roles, namely, the Infrastructure Provider (InP), the Service Provider (SP) and the VDC consumer.

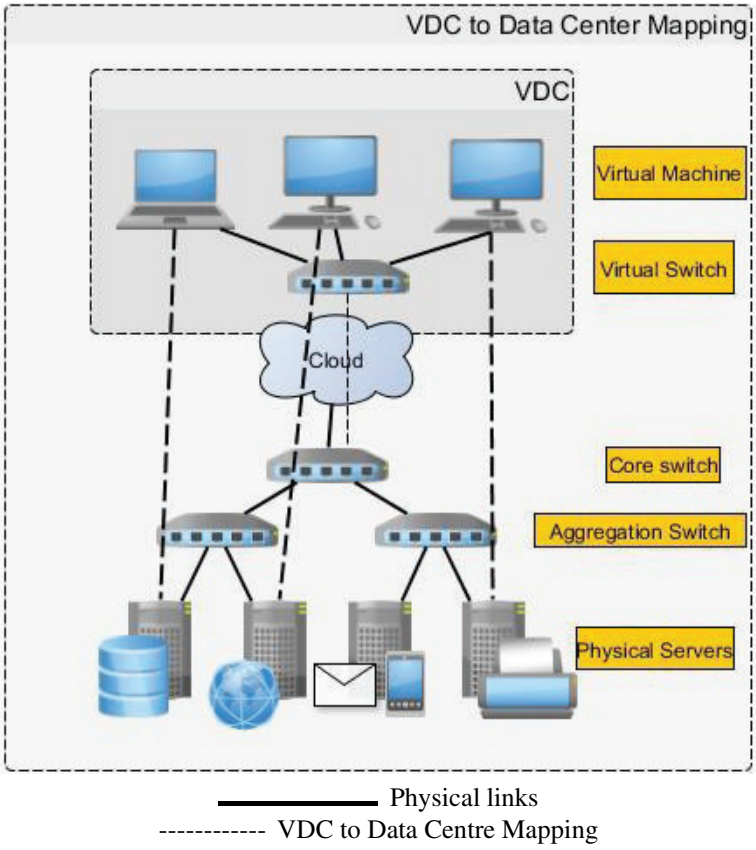


**Figure 1** Mapping of VDC request to datacentre.

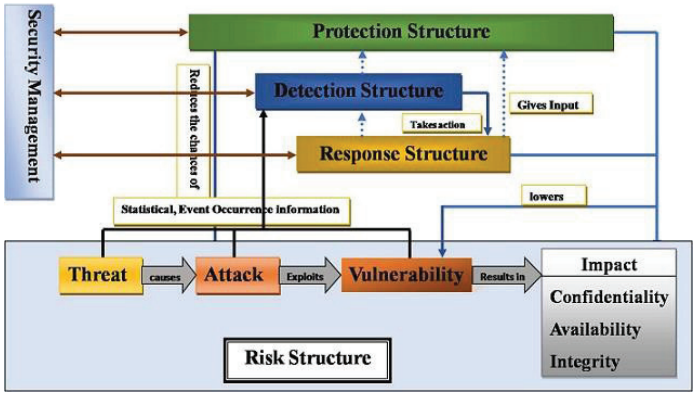


**Figure 2** General Security model for a classic data centre.

**Infrastructure Provider (InP):** The InP provides computing resources, including the associated storage and network resources. These resources are offered to customers via the self-service model in an automated way. In the Infrastructure as a Service (IaaS) model, the provider manages the data centre facilities, hardware and virtualization. The OS, middleware and applications are managed by the customer.

**Cloud Service Provider (CSP):** The CSP manages the cloud resources in the Data centre and allocates the VDC resources. The CSP is a fairly trusted party. The CSP issues credentials to the customer, which authenticates the user in the first level. The CSP employs a separate auditing manager to verify credentials.

**VDC Consumer:** An IaaS environment provides cloud consumers with a high level of control and responsibility over its configuration and utilization. The IT resources that are provided by the IaaS are normally not pre-configured, and the administrative tasks are placed directly upon the cloud consumer. Cloud consumers use this model that requires a high level of control over the cloud-BASED environment.

## 3.3 Secure Anonymous Authentication Algorithm for VDCs

In this proposed algorithm, we mainly focused on anonymous authentication to preserve the privacy of the users. In our scenario, the sender and the receiver can be designated as the cloud user and the Infrastructure provider, and vice-versa. Many times, revealing the senders' personal identities is

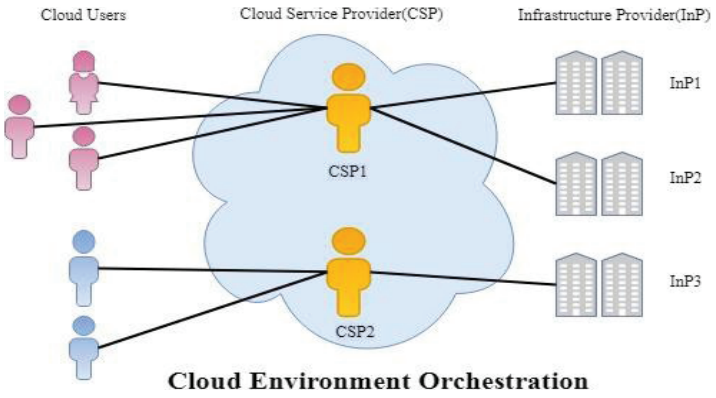


**Figure 3** Cloud user environment.

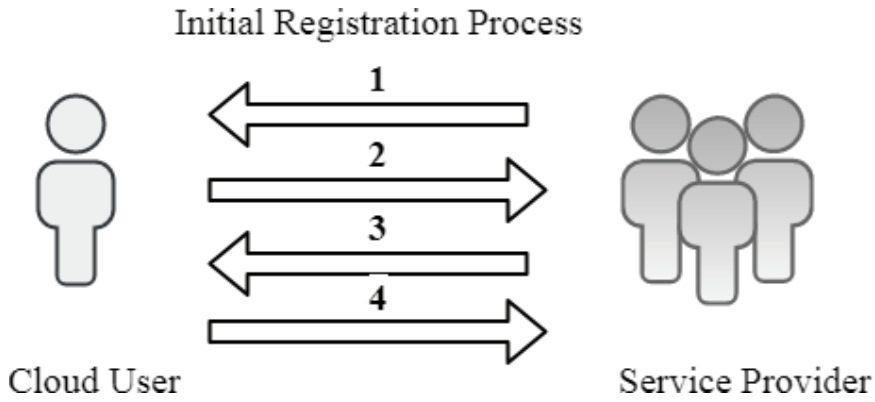


**Figure 4** Customer registration to cloud.

hazardous. The proposed algorithm eliminates the issue of non- repudiation and not revealing senders' identities, i.e., anonymous authentication.

In Figure 3, the cloud user first sends the request to the InP to initialize the anonymous authentication. After receiving the request from the cloud user, the InP performs the anonymous authentication protocol to authenticate the cloud user. The anonymous authentication protocol is explained as follows. The following section consists of the registration phase and the anonymous authentication phase.

### 3.3.1 Registration Phase

Identity and Access Management (IAM) is the security regulation that enables the right individuals to access the right resources at the right times. Enterprises conventionally used on-premises IAM software to manage the identity and access policies of the cloud users. However, currently, as companies add more cloud services to their environments, the process of managing identities is getting more complicated. Therefore, adopting cloud-based Identity management solutions becomes a logical step.

Cloud users are created in the unified cloud directory and then connected to the cloud IT resources that they want to access, including cloud servers and IaaS-based applications. This aspect of cloud computing management is absolutely crucial since it ensures that the right people have the right levels of access to ensure the productivity and increase the security for an InP.

Therefore, it is essential for the cloud users to be registered to access the cloud resources. In this registration phase as shown in Figure 4, the user credentials are acquired by the Infrastructure Provider. The user gives their name, organization, user id and public key for authentication.

### 3.3.2 Master key Derivation Process

Each Cloud Service Provider owns its Provider Master Keys (PMK). These keys generate exclusive keys through derivation for each communication with the customer. The triple DES algorithm is used to derive the key.

### 3.3.3 Customer Master Key (CMK) Derivation Process

The Master Key Derivation method takes the Pseudo Customer Id, the Location TimeStamp (LTS), and a 16-byte Provider Master Key (PMK) as the inputs, and produces a 16-byte Customer Master Key (CMK).

Input Data: Cloud Customer Id i.e., Pseudo Customer Id (PCI), Location TimeStamp (LTS), and PMK (Provider Master Key)

Output Data: Customer Master Key (CMK)

1. $Y = PCI \| LT$; ($\|$ concatenation operation)
2. $Z_L = DES3(PMK)(Y)$
3. $Z_R = DES3(PMK)((Y) xor('FF' \| 'FF' \| 'FF' \| 'FF' \| 'FF' \| 'FF' \| 'FF' \| 'FF'))$
4. $Z = Z_L \| Z_R$

First, the Pseudo Customer ID(PCI) is concatenated with a Location Time Stamp (LTS) and stored in Y. The triple DES algorithm is applied on the result Y and the Provider Master Key (PMK). The result is stored in ZL. The compliment of Y is computed by performing the XOR operation between Y and 8 FFs and the triple DES algorithm is applied on the result. ZR stores the result. Finally, Z is computed by concatenating ZL and ZR. PCI, LT, ZL, and ZR are 8 Bytes long. Z is 16 bytes long.

The 16-byte Customer Master Key (CMK) is then equal to Z, with the exception of the least significant bit of each byte of Z. The CMK is set to a value that ensures that each of the 16 bytes of the Master Key has an odd number of 1to ensure the odd parity requirements for

DES keys are met. The Customer Master Key Derivation is the middle step in the Key Derivation Process.

**Example:**

1. First, we concatenate the PCI with the LTS.

   (Example: PCI = "12 34 56 78", LTS = "01 90 12 3F FF", and $Y$ = "12 34 56 78 90 12 3F FF 01")

2. The Triple DES algorithm is applied on $Y$. The result is stored in $Z_L$.

3. Again, the Triple DES algorithm is applied on $Y$ after performing an XOR operation between $Y$ and the eight bytes set to $'FF'$. The result is stored in $Z_R$.

4. The concatenation result between $Z_L$ and $Z_R$ is stored in $Z$.

## 3.4 Session Key Exchange Between customer and Cloud Service Provider (CSP)

The exchange of session keys is based on the SSL (Secure Socket Layer) scheme. The Public Key Infrastructure (PKI) binds keys with user identities (PAN and SSN) by means of a Certificate Authority (CA). The PKI uses the hybrid crypto system, i.e., both symmetric and asymmetric key algorithms, and benefits from using both types of encryption. In SSL communications, the server's SSL Certificate holds an asymmetric public and private key pair. The session key created during the SSL Handshake is symmetric between the CSP and the client, which is explained further below.

1. The CSP sends a copy of its asymmetric public key to the cloud client during registration.

2. The Cloud Client creates a symmetric session key and encrypts it with the CSP's asymmetric public key. Then, it sends it to the CSP.

3. The Service Provider decrypts the encrypted session key using its asymmetric private key to obtain the symmetric session key.

4. The CSP and Cloud client now encrypt and decrypt all transmitted data with the symmetric session key, which allows for a secure channel because only the client and the CSP know the symmetric session key and the session key is only used for that session. If the client wants to connect to the same CSP the next day, a new session key would be created.

## 3.5 Anonymous Authentication Phase

In the general scenario, for proper security using Diffie-Hellman, we need a value $g$ such that the order of $\boldsymbol{g}$ (the smallest integer $\mathbf{n} \geq \mathbf{1}$ such that $\boldsymbol{g^n = 1 \, mod \, p}$) is a `multiple` of a large enough prime $\boldsymbol{q}$. If t bits security is used, then $\boldsymbol{q}$ must be 2t bits. Since `n` necessarily divides $\mathbf{p - 1}$, $\boldsymbol{q}$ divides $\mathbf{p - 1}$.

## 3.6 Preliminaries and Notations

### 3.6.1 Primitive Root

The primitive root 'g' of a prime number is one such that p and $g$ are co–prime. I.e., the Greatest Common Divisor $GCD(p, g) = 1$ and it is congruent to a *power of g modulo n(gk mod n)*. Every prime number has primitive roots. $k$ is also a prime number.

We say that $g$ is a primitive root of $n$ if g generates all of

$$Z_n^*, \text{ that is, } Z_n^* = \left\{ g, g^2, g^3, \ldots, g^{\varphi(n)} \right\}.$$

Primitive roots can be calculated only for prime numbers based on the Discrete Logarithm for NP-hard problems. Finding the primitive root of the group of primes is hard.

Let $p$ be a prime number. If $b$ is one of the primitive roots of $p$, then the powers of $b$, i.e., $b^1, b^2, b^3, \ldots, b^{p-1} mod p$, generate residual numbers of the prime number $p$. For example, the primitive roots of prime number 5 are 2 and 3.

Any number in $Z_n^*$ will have an order that is one of $2, k, 2k$ or 1. A random number $x$ is chosen and checked if $x, x^2, \ldots x^k \neq 1 (mod \ p)$. If so, then $x$ is a primitive root of $p$; otherwise, the process starts over.

The number of primitive roots is $(k - 1) \approx p/2$ such that the probability of hitting a primitive root is 0.5 in each try.

### 3.6.2 Secret Parameters

To perform this process, let $\alpha, \beta$, and $k$ be the secret random parameters. $k$ is the private key and $g_1^k - Publickey$ $(Discretelogarithm Problem)$ is chosen.

Dummy identifiers are computed to protect the privacy of the sender from other entities in the network.

### 3.6.3 Public Parameters

Let us assume that $q$ is any prime number and $k$ as a Private Key for encryption.

The sender chooses a multiplicative group $Z_q^*$ of order $q$. Then, the sender chooses two random numbers $\alpha, \beta \in Z_q^*$ and a private key $k \in Z_q^*$. The value of $q$ is set as a public parameter.

*$Z_q^*$ is a Primitive group of q. Then, $\alpha, \beta$, and $k$ are selected from $Z_q^*$*

**Table 1** Notations.

| Terms | Notations | |
|---|---|---|
| | Sender Side | Receiver Side |
| Multiplicative group | $Z_q^*$ | $Z_q^*$ |
| Random prime number | $q$ | $q$ |
| Secret Parameter | $\alpha, \beta, k \in Z_q^*$ | $\alpha, \beta, k \in Z_q^*$ |
| Secret Key | $k - Privatekey$ | $k - Privatekey$ |
| Primitive root | $g_1$ | $g_1$ |
| Public Parameter | $g_1^k$ | $g_1^k$ |
| Secret parameters | $D_1, D_2, D_3$ | $D_1, D_2, D_3$ |
| Dummy Parameters | $D_1', D_2', D_3', D_4'$ | $D_1'', D_2'', D_3'', D_4''$ |
| Anonymous Challenger ($C$) | $C = H(M\|D_1\|D_2\|D_3)$ | $C' = H(M\|\|D_1''\|\|D_2''\|)$ |
| Justification | If $C$ equals $C'$, then the message is from an authenticated user. | |

## 3.7 Sender Side Parameter Generation

The sender first computes the public key $g_1^k$, where $g_1$ is the primitive root of the multiplicative group $Z_q^*$. Then, the sender computes the parameter $D_1, D_2$ and $D_3$ for the purpose of anonymous authentication such that

$D_1 = g_1^{\alpha+k}$, $D_2 = g_1^{\alpha+\beta}$, and $D_3 = g_1^{\alpha+\beta+k}$ where $D_1$, $D_2$, and $D_3$ are the sender's secret parameters.

Then, one anonymous challenger $C$ is set to verify the data that are transmitted over the third-party channels.

$$H(M\|D_1\|D_2\|D_3)$$

Moreover, the sender computes the dummy parameters $D_1'$, $D_2'$, $D_3'$ and $D_4'$ as follows.

$$D_1' = g_1^{\alpha+2\beta}$$
$$D_2' = g_1^{-\beta+k}$$
$$D_3' = g_1^{-\beta}$$
$$D_4' = g_1^{-k}$$

The sender sends $C$ and $M$ and the dummy parameter values to the receiver. Finally, the sender sends $\{C\|M\|D_1'\|D_1'\|D_3'\}$ to the receiver to prove its legitimacy.

## 3.8 Receiver Side Verification

By receiving $\{C\|M\|D_1'\|D_1'\|D_3'\}$ from the sender, the receiver needs to check the legitimacy `altered` of the sender. To check the senders' legitimacy; the receiver computes its own dummy parameters $D_1''$, $D_2''$, $D_3''$, and $D_4''$. Then, it computes the value $C'$ such that $C' = H(M\,||D_1''||)D_2''\|D_3'')$. If $C = C'$, then the receiver considers the sender to be legitimate user. Otherwise, the message is discarded.

The receiver computes their dummy parameters and $C'$ using the parameters received from the sender to verify the privacy.

$$D_1'' = D_1' x D_2' x D_3'$$
$$D_2'' = D_1' x D_2' x D_4'$$
$$D_3'' = D_1' x D_2'$$
$$C' = H(M||D_1''||D_2''\|D_3'')$$

If $C$ and $C'$ are equal, then the privacy of the sender is preserved and the message is from an authorized person.

## 3.9 Proof of Concept

The proposed algorithm can be proved by calculating the product of the dummy parameters. This yields the senders actual parameters.

$$\begin{aligned}
D_1'' &= D_1' x D_2' x D_3' \\
&= g^{\alpha+2\beta} x g_1^{-\beta+k} x g_1^{-\beta} \\
&= g_1^{\alpha+2\beta-\beta+k-\beta} \\
&= g_1^{\alpha+k} \\
&= D_1 \\
D_2'' &= D_1' x D_2' x D_4' \\
&= g_1^{\alpha+2\beta} x g_1^{-\beta+k} x g_1^{-k} \\
&= g_1^{\alpha+2\beta-\beta+k-k} \\
&= g_1^{\alpha+\beta} \\
&= D_2 \\
D_3'' &= D_1' x D_2' \\
&= g_1^{\alpha+2\beta} x g_1^{-\beta+k} \\
&= g_1^{\alpha+\beta+k} \\
&= D_3
\end{aligned}$$

The above proof shows the computation of sender's secret parameters by using the dummy parameters received from the sender.

# 4. SECURITY ANALYSIS

This section evaluates the security strength of the proposed algorithm against the theft of customers' identities and unauthorized data access from the data centre through public networks.

## 4.1 User Anonymity

Our algorithm uses secret parameters or pseudo parameters to verify the user information. The hackers cannot be able to attack the communication channel to access the information. The identities of the sender and receiver are kept highly confidential. It is impossible to identify the actual senders and receivers of

the message or data over the public network. $\alpha$, $\beta$, and $k$ are the secret parameters that make deciphering complicated for hackers. $Privatekey(g_1^k)$ ensures the confidentiality of the senders' identities. Therefore, the outside hackers cannot identify the credentials of the senders from a cipher message since it uses only pseudo identities. It is helpful to examine the different methods of adversarial attacks on privacy-transformed data, which helps to create more efficient privacy-transformation methods.

### 4.2 Man-in-the-Middle-Attack

A man-in-the-middle-attack is a form of active eavesdropping in which a middle man controls the entire communications between the victims. This attack is generally possible against any conversation using public-key technology. Our proposed scheme protects the end users' real identities and sends only dummy identities. The dummy parameters are computed using the secret key of the sender. The attacker finds it difficult to identify the message from his intended victim.

### 4.3 Dictionary Attack

Dictionary attacks are prevented locally through delayed response and account locking measures. In a cloud environment, our algorithm protects the real credentials and dynamically computes and sends parameters. It is impossible to dynamically guess the computed dummy parameters.

### 4.4 Privacy Preservation

In all the situations, the identity of the user is preserved during the communication process. Only dummy parameters are sent and verified for user authentication and the authorization services of the cloud user. The intruder is unable to trace the identity if pseudo parameters are sent.

### 4.5 Computational Complexity

The main important part of our solution is the Anonymous Authentication phase. In this phase, a user communicates a service request to a Cloud Service Provider (CSP) with its dummy parameters. The computation process on the user side is marked as the Authentication process. The computation process on the CSP side is denoted as the Verification process. We have measured the total time of the Authentication process and the Verification process. The computation time for the authentication and verification processes takes an average of 2 seconds.

## 5. CONCLUSION & FUTURE WORK

Security is a major threat to computing and storage environments. Providing security for VDCs is a challenging issue. In this article, we proposed a novel privacy preservation algorithm to provide secure access to data centres in the cloud environment. This paper can further be extended by using longer keys to strengthen the information access. Due to the complexity of the hash functions, the computation time that is required for existing privacy preservation algorithms increases as the key size increase. Whereas, the computation times of Primitive root algorithms are found to be comparatively less. With a key size of $2 \times 64 = 128$ bits, our algorithm is found to be complex to attacks. We have shown that the failure to achieve user anonymity is due to vulnerability to man-in-the-middle attacks. We anticipate that the similar security flaws that are identified in this work can be prevented in the future design of anonymous authentication schemes. Our proposed scheme protects user anonymity against any third parties other than the home agent and is also secure against offline dictionary attacks and man-in-the-middle attacks.

## REFERENCES


1. Zhen Chen, Wenyu Dong, Hang Li, Peng Zhang, Xinming Chen, & Junwei Cao. (2014). Collaborative network security in multi-tenant data center for cloud computing. Tsinghua Science And Technology, 19(1), 82–94.
2. Berger, S., Caceres, R., Goldman, K., Pendarakis, D., Perez, R., & Rao, J. et al. (2009). Security for the cloud infrastructure: Trusted virtual data center implementation. IBM Journal Of Research And Development, 53(4), 6:1–6:12.
3. T. A. Syed, S. Musa, A. Rahman, S. Jan (2015). Towards secure instance migration in the cloud, Cloud Computing (ICCC) 2015 International Conference on, pp. 1–6, 2015.
4. Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). Toward Secure and Dependable Storage Services in Cloud Computing. IEEE Transactions on Services Computing, 5(2), 220–232.
5. X. Wang, J. Zhang, M. Wang, L. Zu, Z. Lu, J. Wu,(2014). CDCAS: A Novel Cloud Data Center Security Auditing System", International Conference on Services Computing (SCC), pp. 605–612.
6. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592.
7. Chang, V., & Ramachandran, M. (2016). Towards Achieving Data Security with the Cloud Computing Adoption Framework. IEEE Transactions on Services Computing, 9(1), 138–151.
8. S. R. Talper, T. Kechadi,(2016). A Survey on DDoS Attaks: Router-Bassed Threats and Defense Mechanism in Real-World Data Center", Proc. 2016 Future Technologies Conf., pp. 978–984.
9. Lee, E. (2015). Cooperative Virtual Data Center: Sharing Data and Resources among Multiple Computing Entities. International Journal of Software Engineering And Its Applications, 9(11), 137–152.
10. Mollah, M., Azad, M., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. Journal Of Network And Computer Applications, 84, 38–54.
11. M. Ali, S. U. Khan, A. V. Vasilakos, (2015). Security in Cloud Computing: Opportunities and Challenges, Information Sciences
12. I. El Mir, D. S. Kim, A. Haqiq, (2015). Security modeling and analysis of an intrusion tolerant cloud data center, Complex Systems (WCCS). Third World Conference on, pp. 1–6.
13. Liu, S., Cai, Z., Xu, H., & Xu, M. (2015). Towards security-aware virtual network embedding. Computer Networks, 91, 151–163.

14. Wang, Y., Chau, P., & Chen, F. (2016). Towards a secured network virtualization. Computer Networks, 104, 55–65.
15. Calero, J., Edwards, N., Kirschnick, J., Wilcock, L., & Wray, M. (2010). Toward a Multi- Tenancy Authorization System for Cloud Services. IEEE Security & Privacy Magazine, 8(6), 48–55.
16. Ni, Q., Bertino, E., Lobo, J., Brodie, C., Karat, C., Karat, J., & Trombeta, A. (2010). Privacy-aware role-based access control. ACM Transactions On Information And System Security, 13(3), 1–31.
17. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling data in the cloud: outsourcing computation without outsourcing control. *CCSW*.
18. Khan, M. A. (2016). A survey of security issues for cloud computing. J. Network and Computer Applications, 71, 11–29.
19. Singh, Saurabh & Jeong, Young-Sik & Hyuk park, Jong. (2016). A Survey on Cloud Computing Security: Issues, Threats, and Solutions. Journal of Network and Computer Applications.
20. Kritikos, K., Kirkham, T., Kryza, B., & Massonet, P. (2017). Towards a security-enhanced PaaS platform for multi-cloud applications. Future Generation Comp. Syst., 67, 206–226.
21. Zhou, H., & Ren, J. (2014). A secure virtual data center based on data labeled cloud-agent. IEEE 5th International Conference on Software Engineering and Service Science, 937–940.
22. Iankoulova, I., & Daneva, M. (2012). Cloud computing security requirements: A systematic review. 2012 Sixth International Conference on Research Challenges in Information Science (RCIS), 1–7.
23. Almutairi, A., & Ghafoor, A. (2014). Risk-Aware Virtual Resource Management for Multitenant Cloud Datacenters. *IEEE Cloud Computing*, 1, 34–44.
24. Tupakula, U. K., Varadharajan, V., & Akku, N. (2011). Intrusion Detection Techniques for Infrastructure as a Service Cloud. 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, 744–751.
25. Almutairi, A., Sarfraz, M. I., Basalamah, S. M., Aref, W. G., & Ghafoor, A. (2012). A Distributed Access Control Architecture for Cloud Computing. IEEE Software, 29, 36–44.
26. Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *J. Network and Computer Applications*, 79, 88–115.
27. Modi, C., Patel, D., Borisaniya, B., Patel, A. & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. The Journal of Supercomputing, 63(2), pp. 561–592.
28. Ramachandran, M. (2016). Software security requirements management as an emerging cloud computing service. International Journal Of Information Management, 36(4), 580–590.
29. S. Namasudra, P. Roy, P. Vijayakumar, S. Audithan, B. Balusamy,(2016). Time efficient secure DNA based access control model for cloud computing environment, Future Generation Computer Systems 73, 90–105, 2017.
30. Ramachandran, M., & Chang, V. (2016). Towards performance evaluation of cloud service providers for cloud data security. International Journal of Information Management, 36(4), 618–625.
31. Li, Y., Gai, K., Qiu, L., Qiu, M., & Zhao, H. (2017). Intelligent cryptography approach for secure distributed big data storage in cloud computing. Information Sciences, 387, 103–115.
32. Batista, B.G., Ferreira, C.H., Segura, D.C., Filho, D.M., & Peixoto, M.L. (2017). A QoS- driven approach for cloud computing addressing attributes of performance and security. Future Generation Comp. Syst., 68, 260–274.
33. A. Chonka, Y. Xiang, W. Zhou, A. Bonti, "Cloud security defence to protect cloud computing against http-dos and xml-dos attacks" in Journal of Network and Computer Applications, Elsevier, vol. 34, no. 4, pp. 1097–1107, 2011.
34. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2017). A dynamic prime number based efficient security mechanism for big sensing data streams. Journal of Computer Systems Science, 83, 22–42.