International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Smart Resilient Security Framework and Solutions for Cloud-driven Digital Supply Networks

Kathiravan Srinivasan, Takshi Gupta, Senthil Kumaran S, Srinivasan N

Abstract: ***The cloud-based logistics services allow cost reduction, higher elasticity, flexibility, and maximum utilization of resources for performing high computations and data analytics. Logistics and security are complex issues with the corporate entities when these are to be used for taking critical issues. To understand these, this paper discusses a conceptualized, flexible security framework for cloud-driven digital supply chain in Agricultural. Moreover, a security enhancement layer is included at each layer of the cloud with a feasibility study on protecting user information in the logistics services ambiance. Also, the Data Residency for cloud-based logistics services is elaborated with Data Security analysis. Further, the article discusses the possible solutions to handle the security concerns of the logistic model.***

Keywords: Agriculture Supply Chain, Security, Cloud Network

I. INTRODUCTION

Non In recent years, the development of cloud computing has been considered as a unique feature among the key progresses in the area of computing. The distribution of quick, reasonably-priced and scalable services to people and corporate establishments is referred to as cloud computing. It is a ground-breaking standard that expedites the clienteles to implement their project operations and also aides to store the information in the third-party possessed servers. Since the implementation of cloud computing standards has several benefits like pliability, universal availability, convenience, easy maintenance, and economic pay-per-use billing models for corporate entities [1] [2]. The cloud computing services are divided into three major categories, software as a service (SaaS), Platform as a Service (PaaS), and infrastructure as a service. The applications are running in the cloud are known as SaaS, and it presents an architecture that can run several instances of itself regardless of location. PaaS is a platform that enables developers to write applications to run on the cloud. This would have various applications that can be deployed instantly. The last category is infrastructure as a service that can be accessible by internet technologies and shares the computing infrastructure. The sharing resources are like servers, storage, security, databases, etc. Four different models are suggested in cloud computing. The first model is the public deployment model in which the third parties or any organization operated and distribute services to the public domains. The second is the private model, which is owned and operated by the organization and severed for their internal users. The third model is a community model which operated and organized for specific communities. The last model is a hybrid, which is a mixture of two or more clouds [3][4][5][51][52]. These providers also account for modern-day networks, such as 5G, Internet of Things, as well as novel allocation strategies for handling diversified services [6][7]. Mostly, the Cloud Service Providers are responsible for handling and functioning of the Public cloud infrastructure [51]. Furthermore, it is accessed by an extensive assortment of registered clienteles, and the CSP is liable for the configuration and organization of these services. While considering the private cloud infrastructure, it is handled and functioned by either the CSP or clienteles. However, in some particular scenarios, both the CSP and clienteles are involved in handling and managing the private cloud infrastructure that is owned by a solitary client. The community cloud infrastructure is catered for the needs and utility of a particular selective cluster of establishments. The hybrid cloud is the amalgamation of several disparate cloud models like the public, private and community exemplars for providing tailored infrastructure utilities depending on the needs of an establishment or institution [8][9][10][11].

The organizations can evade a conciliation of their functioning efficacy by implementing the cloud associated infrastructure for swiftly enhancing, successfully recognizing and utilizing the scientific elucidations [12]. Amongst the corporate entities, the private and public cloud associated elucidations are mutually attaining prominence. Nevertheless, as a result of witnessing the goals of the business entities and also considering the cost-to-serve metrics, it can be observed that solely the private cloud models are contending with the predominantly available public cloud models. Additionally, hybrid clouds are designed and tailored based on the specific necessities of corporate organizations. Furthermore, for constructing a hybrid cloud model, at least a solitary public and a single private cloud infrastructure are essential. Moreover, based on the necessities of corporate enterprises, numerous public and private cloud services can be amalgamated together to build a hybrid cloud infrastructure. Besides, the hybrid cloud services are a seamless and an equilateral blend of both the exterior and interior assets that offer a perfect fusion of swiftness, cost leadership, dynamism and service-levels [13].

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author

Kathiravan Srinivasan*, Department of Information Technology, School of Information Technology and Engineering, Vellore Institute of Technology (VIT), Vellore, Tamil Nadu, India. Email: kathiravan.srinivasan@vit.ac.in

Takshi Gupta Information Security Engineering Department, Soonchunhyang University, Asan-si, South Korea-31538.Email: takshi_gupta2012@hotmail.com

Senthil Kumaran S Department of Manufacturing Engineering, School of Mechanical Engineering, Vellore Institute of Technology (VIT), Vellore, Tamil Nadu, India. Email: senthilkumaran.s@vit.ac.in

Srinivasan N Department of Manufacturing Engineering School of Mechanical Engineering, Vellore Institute of Technology (VIT), Vellore, Tamil Nadu, India. Email: srinivasan.narayanan@vit.ac.in

Therefore, hybrid cloud services seem to be the finest and appropriate infrastructure for Logistics Services.

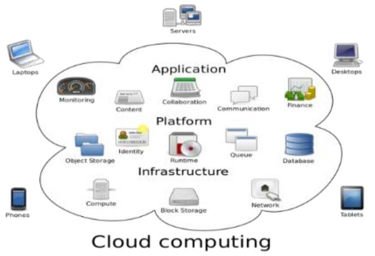


Fig. 1 An illustration of a Cloud Architecture

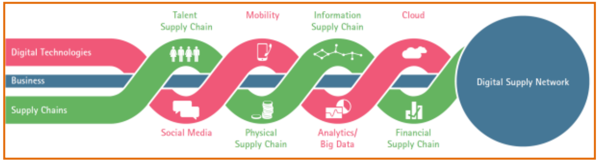


Fig. 2 Cloud and supporting technologies deployment in logistics and supply chain networks [17].

Based on Gartner Inc, 2016 reports [5], the hybrid cloud infrastructure will be replacing the existing private cloud services. Furthermore, the report suggests the fact that during the completion of 2017, nearly fifty percent of the business organizations will switch over to hybrid cloud services. Cloud computing architecture, as described in Fig 1, indicating the essential required components in cloud computing. The cloud computing architecture composed servers, storage, networks, and clients. The cloud-based delivery is conducted between the front end platforms (clients, mobile devices) and backend platforms (servers, storage) through the network. Fig. 2 demonstrates the cloud and supporting technologies deployment in logistics and supply chain networks [14]. Fig. 3 illustrates the cloud computing architecture used in logistics services and its visual model is presented in Fig.4.

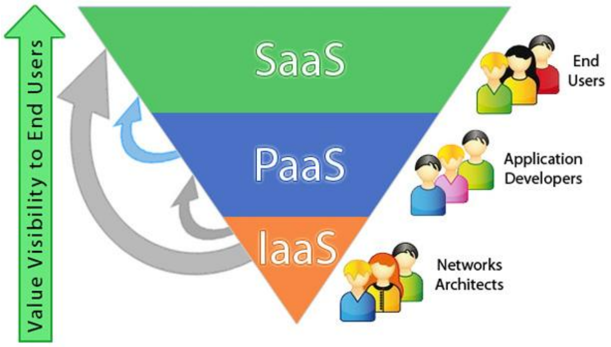


Fig. 3 Cloud Architecture for Logistics Services.

In general, the logistics networks are complex structures created by offering valuable services to the final consumer or business entities [13-15]. This network primarily focuses on the exchanges and movement of material and information amongst the business enterprises. Also, the logistics network is a highly intricate edifice in which the business entities can be connected, with mutual communication amongst each other; and the word chain signifies a modest chronological group of associations. Moreover, the logistics networks enable the corporate entities to differentiate amongst the worthiness of building partnerships and the notion of combined efforts for attaining a better final consumer fulfillment. Lately, the implementations of cloud infrastructure based logistics networks have achieved a significant status among the business firms for enhancing the competence of these networks. Besides, the logistics networks that are integrated with the cloud infrastructure will be facilitating the critical processes such as logistics planning, purchase orders, tracking and monitoring, delivery and so on, and at the same time, the overall efficiency of the processes will also be enhanced. Cloud-based logistics technology is more effective in comparison to the traditional means of data as it facilitates the sharing of information much more comfortably and faster [16].

The following are some generic advantages due to the utilization of cloud infrastructure in logistics networks

a) Agile operations of the corporate entities: Primarily, the most significant advantage achieved using deploying the cloud infrastructure is the agility in the operations of the corporate enterprises. This scenario ascends because of secured data management and end-to-end amalgamation. Further, in any logistics network, the corporate enterprises attempt to execute several commercial operations, which may be widely divergent. However, certain operations are based on vital data that is part of everyday corporate tasks. Conversely, the public cloud infrastructure can be deployed if the data utilized is not so vital. Besides, vital operations can be executed by employing private cloud services. Also, the corporate entities can surpass the security issues and can also control their assets using broadening their requirements.

b) Cost optimization and leadership: The cost-leadership is the other main advantage of deploying cloud infrastructure in logistics networks. Additionally, this leads to the lessening of the overall expenditure. Moreover, based on the corporate tasks and its requirements, the enterprises can devise and decide upon the usage portion of the public and private cloud services in the hybrid cloud infrastructure. The vital tasks are relatively scarcer. Therefore the functioning expenses get significantly lessened due to the scalable facilities in cloud infrastructure. Subsequently, the cloud amenities possess the capability to scale rapidly and competently between the distributed data centers of the cloud at a cheaper rate than buying a lavish apparatus or leasing the massive data centers with permanent infrastructure.

c) Augmented security and disseminated task-force: In general, security and data integrity are two fundamental apprehensions, while deploying a public cloud. On the contrast, better security can be realized by using hybrid cloud infrastructure services. Therefore, corporate entities can achieve superior security to their operational practices using retaining the data away from the public cloud network. Moreover, the operational expenditure can be decreased by making the routine to perform effortlessly across diverse ambient settings. Additionally, the hybrid cloud services provisions a disseminated task-force by employing the primary security features that can be amalgamated with the business data centers to guarantee data integrity. Furthermore, it can be ascended between manifold exterior elucidations to safeguard consistency and also to offer higher availability.

d) Improved functioning and operation: The corporate entities might achieve supreme throughput by augmenting the available possessions of their commercial practices. Moreover, while considering the scenario of the business organizations, the service level agreement can be enhanced, and outage duration can be decreased by deploying the exceptionally scalable system. These systems provide the necessary dexterity and are believed to be dynamic.
e) Corporate firms and its international influence: Normally, the business firms can be connected with the external merchants through the cloud network, which improves the efficiency of the supply chain network. When essential, vertical scaling can be achieved as a result of the flexibility in the functioning of the cloud network. This scenario can further augment the modeling, imagining, and scheming of the amenities.

This paper incorporates a security framework for cloud-based logistics services, which enables an organization to implement its logistics services securely. A security enhancement layer is included at each layer of the cloud with a feasibility study on protecting user information in the logistics services ambiance. In section II, the related work is presented. In Section III the data residency for cloud-based logistics services is elaborated and Data Security analysis presented in Section IV. Section V gives solutions to the problems, and finally, Section VI concludes the paper.

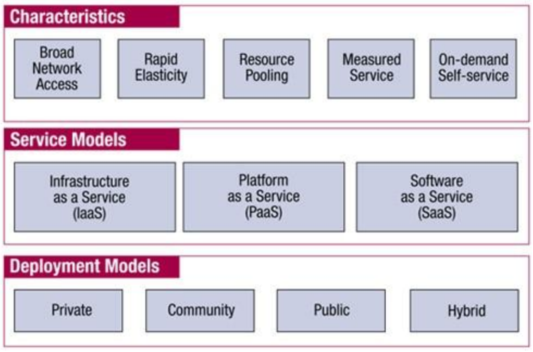


Fig. 4: Visual Model of Cloud Computing.

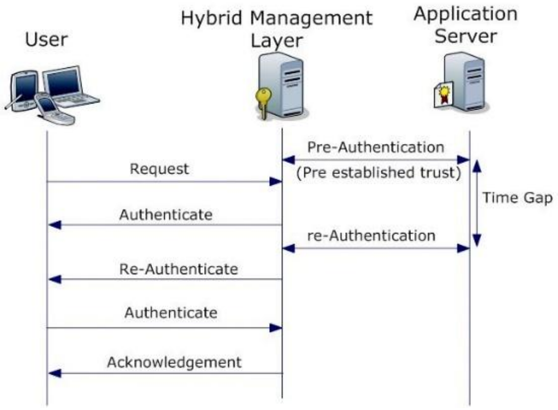


Fig. 5 An overview of entities involved in authentication [17].

II. RELATED WORK

Cloud computing supports various business organizations through high financial savings. The cloud provides streamline processes of the enterprise with adequate productivity and transforming business processes and reducing the cost. The cloud computing helps in business to attain scalability, more satisfied customers and provide reliable backups. In the era of cloud computing, various researches have been conducted to enhance the facilities of cloud-driven networks. Uchenna et al. [31] gave a cloud-based virtual organization framework that Integrates Cloud Computing Model (CCM) with the Virtual Value Creation (VVC) framework of Virtual Organization (VO) to improve traditional methods of business. Mushtaq et al. [32] focused on information security in cloud computing. The authors focused on secure data transmission, encryption of data and it is Processing, Secure database, Shell, and logs in the clouds. Ukil et al. [33] give a security framework to manage the cloud system more efficiently and provide security and mitigate threats. Tawalbeh et al. [34] suggested cloud computing framework in which the data is classified based on the importance and important data is encrypted. Arjunan and Modi [35] suggested an intrusion detection system for clouds based on signature and anomaly-based techniques. The IDS helps to identify various attacks in the cloud. Marwan et al. [36] suggested a secure framework for cloud-based medical image storage in which segmentation and watermarking mechanisms are used to provide privacy in the saving of a medical image. Al-Bahadili et al. [37] suggested Cloud Collaborative Commerce (cc-commerce) model to Supports cost-effective computing resources for businesses and reduce installation and running costs, delay, Security, etc. Tawalbeh et al. [38] presented the secure mobile cloud computing framework which used trust delegation technique to provide better security and performance. The state-of-the-art comparison of existing approach for cloud-driven networks is presented in Table 1. Some other research works to follow are, cloud computing governance [39], securing the cloud-Governance[40, big data fraud detection[41], single sign-on for clouds[42], proactive user-centric security[43], preventing insider cyber threats[44], authentication and authorizations[45], email spam prevention in logistics[46], proxy network formations[47], firewall management[48][49]and big-traffic evaluations [50].

Table. 1 The state-of-the-art comparison of existing approach for cloud driven networks.

Scheme	Authors	Key Contributions	Logistic Net works	Security Consideration
Cloud-based virtual organization framework	Uchenna et al.[31]	Integrates cloud computing model (CCM) with the Virtual Value Creation(VVC)Framework of Virtual Organization (VO) to improve traditional methods to business	No	No
Framework for information security	Mushtaq et al. [32]	Secure data transmission, Encryption of data and its Processing, Secure database, Shell and logs	No	Yes
Security Framework for clouds	Ukil et al. [33]	Manage the cloud system more efficiently and provide security and mitigate threats	No	Yes
Cloud computing framework	Tawalbeh et al. [34]	Importance based classification of the data and encrypt essential data	No	Yes
Cloud IDS	Arjunan and Modi[35]	Combines signature and anomaly-based techniques to detect various attacks	No	Yes
Secure Framework for Cloud-Based Medical Image Storage	Marwan et al. [36]	Segmentation and watermarking mechanisms are used to provide privacy in the saving of medical image	No	Yes
Cloud collaborative commerce (cc-commerce) model.	Al-Bahadili et al. [37]	Supports cost-effective computing resources for Businesses, and reduce installation and running costs, delay, Security etc.	No	Yes
Secure mobile cloud Computing framework	Tawalbeh et al. [38]	Used trust delegation technique to provide better security and performance	No	Yes

III. PROPOSED SECURITY FRAMEWORK

The security framework for the cloud-based logistics services is provided in three aspects. The first includes role management and privilege modeling provided by the API at the SaaS layer, second includes the security using isolation policies provided by the PaaS layer, and third includes security using authentication over servers using IaaS layer. In general, a user interacts with the application, which authenticates and provides security at all the layers of the cloud. This process is further abstracted and improved as the hybrid cloud management platform pre-authenticates itself with the PaaS and IaaS layers. The user only validates itself to the hybrid management layer without sending any information back to the servers. Further, this prevents overheads and latency involved in the authentication mechanisms.

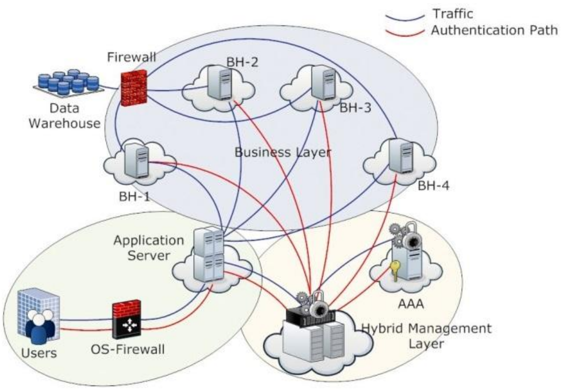
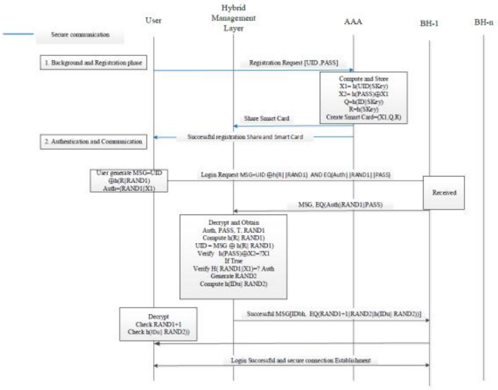


Fig. 6 An overview of the authentication mechanism for the security framework for cloud-based logistics services.

A simple model presenting security enhancement via a hybrid cloud management layer is shown in Figs. 5 and 6. The layer is responsible for running all the authentication protocols in collaboration with the underlying cloud system. The logistics services only authenticate the user to the upper layer and do not send or retrieve user security policies from the underlying infrastructure layer. However, for distributed security management, a new authentication server layer can be added to the hybrid layer. This server layer can interact with the security policies of different cloud components to ensure user authentication, privacy, integrity, and confidentiality. A user only re-authenticates, if the hybrid cloud management systems re-authenticates itself with the authentication server during the same session.

The detailed procedures formed on the backbone of the ideology presented in Fig.6are shown in Fig.7. From the figure, it can be noticed that there can be multiple Business Houses (BH), which support cloud services to a user and rely on a hybrid management layer for the security of communication as well as for the management of the services used by their respective user. The hybrid layer can be virtually formed similar to a typical exchange or can be deployed separately for each BH.

However, a standard operation interface is required for separately operating hybrid management layers as all the decisions on the authentication of a user are to be shared with other BHs. Further, this helps to identify a user who is legitimate for operations over a given cloud infrastructure. All these operations of the user-accessibility to cloud-based logistics services are performed by the logistic-exchange authentication protocol presented in Fig. 7. The protocol helps to authentication as well as disseminates cloud services by following priority accessibility to each BH.


User
Hybrid Management Layer
AAA
BH-1
BH-n
Secure communication
1. Background and Registration phase
Registration Request [UID ,PASS]
Compute and Store
X1= h(UID||SKey)
X2= h(PASS)⊕X1
Q=h(ID||SKey)
R=h(SKey)
Create Smart Card=(X1,Q,R)
Share Smart Card
Successful registration Share and Smart Card
2. Authentication and Communication
User generate MSG=UID ⊕h(R||RAND1) Auth=(RAND1||X1)
Login Request MSG=UID ⊕h(R||RAND1) AND EQ(Auth||RAND1||PASS)
Received
MSG, EQ(Auth||RAND1||PASS)
Decrypt and Obtain
Auth, PASS, T, RAND1
Compute h(R|| RAND1)
UID = MSG ⊕ h(R|| RAND1)
Verify h(PASS)⊕X2=?X1
If True
Verify H(RAND1||X1)=? Auth
Generate RAND2
Compute h(IDu|| RAND2)
Decrypt
Check RAND1+1
Check h(IDu|| RAND2))
Successful MSG[IDbh, EQ(RAND1+1||RAND2||h(IDu|| RAND2))]
Login Successful and secure connection Establishment

1. Background and Registration Phase: In the background and registration phase, the user registers their unique id and password through a secure channel to the authentication server. After the successful registration, the authentication server issues a smart card to the hybrid management layer and the user with a successful acknowledgment (ack).

2. Login Phase: In this phase, the legitimate user generates a message with the help of a smart card. In the message, the original id is hidden to prevent the man-in-the-middle attack. The login request is forwarded to the Business layer. The Business layer again forwards this message to the hybrid management layer to check its authenticity.

3. Verification Phase: After receiving the message, the hybrid management layer checks and decrypts its id and analyzes its authenticity with the help of the original smart card.

4. After passing through the authentication validation mechanism, the hybrid management layer sends a strong message to the business layer. The business layer accepts the user and considers it as a legitimate operator. Following this, the business layer forwards this message to the end-user. The user checks the authentication by decrypting the message from the business layer.

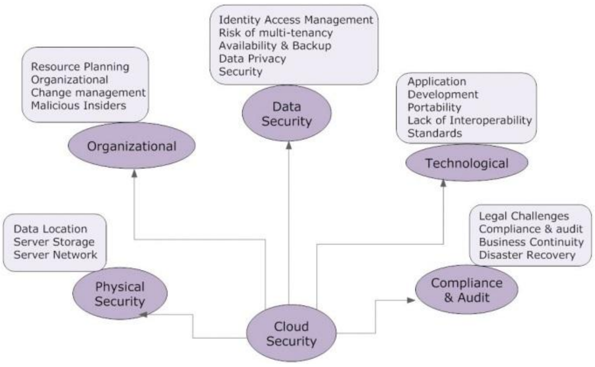


Fig. 8: Cloud Provider Risk Categorization.

Data Residency

The cloud technologies support business organizations to decrease the cost of ownership, increase the scalability and flexibility of IT implementations and support to attain the market objectives. The cloud technologies provide business benefits, but rather than there, and some challenges are associated with data and information (Fig. 8):Access Permissions: Who have the access permissions (modify, delete, add, etc.), and who will manage the data?

Law Regulation for data: what are rules and policies associated with the data storage?

Data Breach: The security parameter which is used to identify the data breach and abnormal modification and how these prevented?

Contract Termination: Will data remain in the cloud even after expiration of services?

Data Encryption and Tokenization

Data encryption and labeling are often referred to as a means of protecting information when transmitted over the Internet or stored statically. Data encryption is a mathematical process that converts plain text into ciphertext and cannot be read by anyone other than the client that holds the encryption key. Encryption is the process of using an algorithm to convert plaintext information into an unreadable form called ciphertext. An algorithm and encryption keys are needed to decrypt the information and return it to its original plain text format. In Tokenization, it converts a meaningful piece of data (such as an account number) into a random string called a token. If there is a violation, the actual data resides locally in the token database; then there is no meaningful value; the token is randomly generated. The value is plain text, and the map is stored in the database.

The main difference in the encryption and tokenization is that tokenization protects against the only external threats whereas the encryption provides security against internal and external threats. The tokenization has to manage with more massive servers and databases, and the complexity is increased with the increase of data volume, but in the case of encryptions, the lightweight server required.

IV. DATA SECURITY AND CLOUD SECURITY

The cloud will have a dramatic impact on how the applications and data can be secured, so in this section, we will discuss how organizations can address some majors cloud security challenges with identity and access management. The cloud in cloud computing refers to the Internet. It helps users to access devices anywhere on the Internet, share files, audio, video, etc., access software and databases through SaaS (software as a service), and release and update users' devices without installing the software. The context-wise categorization of the cloud is public, private and hybrid. As information about the applications moves further from the business organizations the access and visibility of the information are reduced. The cloud service providers pay attention to the performance and scale instead by consider the data security and application security to mitigate the risk probabilities. Most first-generation clouds highlighted the loss of visibility control that can happen when the applications and data move off-premise. A survey is conducted by the Oracle application user group to analyses the significant parameter of the clouds which are the more payable factor in terms of concentrations. The survey concluded that 82% were bothered about data privacy, and 40% were focused on the backend integration challenges. Another study presented by the Ponemon Institute which concluded that 54% of IT professionals were concerned about the security breach due to risk at a cloud provider site.

An online survey conducted by the CSO, among the security professionals which emphasizing the top cloud security concerns. The survey concluded that the primary concerns were all related to mobile data access regulatory compliance and identity management.

The cloud applications are deployed to provide support to mobile users who are moving. The primary issue is how to prevent the data from unauthorized access and reduce the data breaches due to inadequate user authentication and weak passwords.

Cloud computing can be considered as very useful because it provides a centralized data store that contains the user information and crucial data. The key management should be ensured in the cloud that the key should be secure and not found to anyone easily. Insecure Interfaces, APIs and UIs, are the lifeblood of computing connections and integration between users and cloud computing. The IP address of cloud API shows the connection between the user and the cloud. Therefore, as per security perspective, securing API from attacks or error is much needed for cloud security.

The security approach should be considered as an inside-out approach to secure every layer of the stack. Inside-out security refers to the application and data security across all layers and middleware. The risk associated with databases, middleware and application layer is much more than the apply risk mitigations and preventions. The security supports to enable the opportunity with every new cloud initiative application security, and data security is a prerequisite. Various customer risk categories are discussed in Fig.9.

1. Secure data transfer. The internet is a medium of communication on which the traffic between network and services go through the Internet. The surety of a secure channel assures data transmission security. Https is used when a connection is made with the browser to service providers with a URL. Rather than https, the data should be encrypted and verified through standard protocols aims for the protection of internet communications such as Internet Protocol Security (IPsec).

2. Secure software interfaces. The Cloud Security Alliance (CSA) suggests understanding the behavior and working of the software and interface or API's which are used to interact with the cloud services. The weak designing and coding bug of the interface APIs lead to security issues related to confidentiality, integrity, availability, and accountability. CSA recommends that understanding is required that how any cloud provider can integrate security across the entire service, from authorizations, authentication, and access control technologies to activity monitoring strategies.

3. Secure stored data. When the data is on the provider's server and is being used by cloud services, your data should be securely encrypted. In the Q&A: The cloud solution was revealed, and Forrester warned that some of the providers ensure the protection of the data used in the application or the processing of data. Ask potential cloud providers on how to protect the data not only during the transmission but also when the data is on the server and used by the cloud-based applications. Also, check if the vendor handles the data securely, for example by deleting the encryption key.

4. User access control. The data on the cloud server is accessed by the employee of that organizations. The access control on the data is defined based on sensitivity related to data which is accessing by employees. First, the accessibility is given on the basis of requirements and their capability to handle the data, follow research firm Gartner's suggestion to ask to define the specific level of access permission of the peoples.

5. Hacked interfaces and APIs - The probabilities of exploitations of the API are much high due to accessing through the open Internet. The risk is associated due to the weak interfaces and API's in the coding and deployment part of the revels some vulnerability which leads to the attacks on the confidentiality, integrity, availability, accountability and empowers the fraudulent use of cloud services. Most free software trials and registration through cloud applications compromise cloud to malicious users. Various kind of attack on the cloud server like DoS attacks, email spam, automatic click fraud, and pirated content is performed through such kind of vulnerabilities. Therefore, to minimize the attack possibilities, the cloud service provider should adopt a robust incident response framework that helps to provide reliability and security against these issues. Before adopting such a framework, it should better to verify the strength of the framework and monitor in the cloud environment.

6. Shared technology issues in a multi-tenancy environment: The IaaS vendor uses the virtualization concept to deliver the services in the multi-tenant environment. The virtualization has the capability to share resources among multiple users. The malicious user gains information about the legitimate user through the hypervisor in a multi-tenant environment. This vulnerability leads to attack in cloud infrastructures and not designed to offer reliable isolation in a multi-tenant environment. The property of sharing the resources increases the threats to the overall cloud infrastructures [51] [52]. To mitigate such risks, the authentication and authorization mechanism can be used.

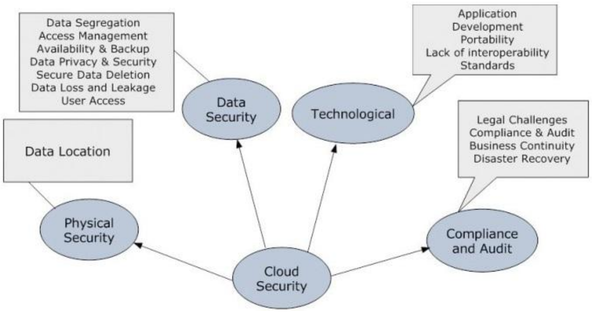


Fig. 9: Customer Risk Categorization

7. Data loss and leakage: cloud computing has the nature of sharing information among multiple users, which leads to the possibility of deletion, alteration, or modifications in the original data. The loss of encoding or decoding keys can also make a data loss.

There are lots of factors which are responsible for the data loss like lack of authorizations, authentications, access control, and weak cryptographic mechanisms, low reliability, and lack of policies for disaster. To prevent data loss form such kind of issues, there are certain solutions are available like Secure API, data integrity, secure storage, secure encryption key and algorithms, and data backup to provide prevention against data loss.

8. Insufficient due diligence: The Cloud Security Alliance (CSA) stated that when executives formulate business strategies, they must consider cloud technology and service providers. In the evaluations of technologies, the roadmap and diligence checklist helps to get the success chances.

Organizations that are eager to adopt cloud technologies and select providers without conducting due diligence face many risks.

9. Advanced persistent threats (APTs): APT is a parasite type of cyber-attack that penetrates the system and gains a foothold in the target company's IT infrastructure to steal data from it. APT has quietly pursued its goals for a long time, often adapting to security measures designed to fend off them. CSA said that once in place, APT can move horizontally through the data center network and converge with normal network traffic to achieve its goals.

10. Meltdown/Spectre: These vulnerabilities may not be materially flawed, but specter and melting pots - to find out how processors handle defects in speculative execution - will cause significant disruption this year. Not patching these vulnerabilities is not an option, and because they exist at the CPU level, patches are more risky and destructive than most patches.

11. Bandwidth cost: High-speed communication channels are directly proportional to the efficiency of cloud computing. The cloud computing can save costs on the software and hardware, but it still required large bandwidth. It is almost without high-speed communication channels; cloud computing services cannot be fully utilized. Migration to the cloud almost eliminates the upfront costs while increasing the data communication cost on the network. It involves data transmission between private and other clouds [18]. If the consumer is prominent, applications are data-intensive, and consumer data is distributed across many clouds (Private/Public/Community). Cloud computing provides lower costs for CPU-intensive operations than data-intensive operations the grey argument - the calculation of the near data "still applies to data-intensive work that is still relevant [19]. In other words, private clouds can be a better platform for data-intensive applications rather than the public/hybrid cloud.

12. Segregation: The multi-tenancy is the main feature of cloud computing because it supports data to store by multiple users in the cloud. The multiple user access at a single time causes the possibilities of the data interruptions. By injecting client code or by using any Applications may invade data. It is, therefore, necessary to store the data separately from the remaining customer data. Use tests such as SQL injection laws, Data to detect or detect data isolation vulnerabilities.

13. Costing Model: Cloud consumers must consider Computing, communication and integration trade-offs. The infrastructure costs can be reduced by adopting the cloud, but it does increase the data communications costs, that is, the cost of transferring organizational data to public and community clouds and the cost per unit of computing resources used may be higher. This issue is particularly prominent if consumers use hybrid cloud deployments Models where organizational data is distributed across multiple public/private (internal IT infrastructure)/community clouds. Intuitively, on-demand calculations apply only to CPU-intensive operations [20].

14. Network Security: It includes Domain Name Server (DNS) Attack, Sniffer Attack, (Internet Reuse) Protocol) IP Network challenges, and related cybersecurity [21]-[25]. DNS for converting domain names to IP addresses but attack users in DNS to route to other than the original cloud. Sender and the receiver reroute through some intruder connections. Sniffer attack is initiated by the application and capture Packets flowing through the network that are not encrypted.

15. Service Governance: In order to achieve business goals, each business unit independently provides services by utilizing external cloud services and even managing its infrastructure. Their success has demonstrated to them the pace of innovation and flexibility from outside of IT, and there will be no repeat customers right now. Today, IT departments are unable to fully control the supply of infrastructure and lift supply and operations. This decentralized ownership increases the complexity of the governance, compliance, and risk management that IT provides to protect its business. IT departments need to find new ways to leverage their business to adopt new cloud technologies while not affecting the flexibility that their internal customers now expect from the cloud. It is evident that “Cloud management platform vendors are struggling to find solutions that help IT departments use traditional operational management tools in conjunction with decentralized cloud platforms” [26]-[27].

16. Service Provisioning: Service configuration is used to support service management. In service management, the resources (such as cloud services) can be allocated to use applications or Web services for a certain period. Moreover, current methods and mechanisms for service provision vary from vendor to supplier. The IT team needs to develop a strategy for considering an important aspect of cloud computing, which can be a set of standard APIs that automate the entire service provisioning cycle from allocation to deallocation [28]-[30]. Although most users of the cloud platform want simpler approaches to copy/paste, the actual configuration of the service is too complex for the average user. Also, the cloud platform vendor's user interface for administrators cannot simultaneously meet the needs of a single server instance customer and a large MNC with hundreds of server instances [31]-[34].

People are worried that cloud computing will create new risks and loopholes. There are new assumptions risks, but the exact nature will depend mainly on the establishment of suppliers. All software, hardware, and network devices are vulnerable. Discover new loopholes through application layer security and well-designed business processes, you can protect the cloud from frequent attacks, even if some of its components are the inherent weakness.

V. SOLUTIONS TO IMPROVE CLOUD SECURITY AND TRANSPARENCY

Cloud security and transparency is an essential factor for those organizations who want to adopt cloud computing facilities. There are specific solutions that help to enhance cloud security and transparency without affecting the performance and service.

- Governance and Compliance: The initial step is to implement a governance solution for access. To address the top compliance issues in the cloud, Oracle's identity portfolio can provide a complete integrated solution with regular application certifications and automated onboarding and off-boarding. The attacks in the cloud can be reduced by maintaining and controlling privileged accounts.

- Fraud Detection: The second thing organizations can do is add fraud detection mechanisms, which help to avoid attacks. Oracle's adaptive access manager provides fraud detection mechanism through anomaly detection and provides context-aware security [40]. For the security perspective, the cloud should be device context-aware, time context-aware and location context-aware.
- Cloud Single Sign-on: Cloud Single Sign reduce the possibilities of password thefts. Weak passwords can lead to a significant loss in the cloud environment or increase vulnerability. Therefore, single sign-on facilitates the security of the cloud by leveraging the performance.
- Authorization to Data and Applications: The fourth thing we can do is add privileges for applications and data with their roles. Centralizing policy management is used for secure application data and transactions in the Oracle's entitlement server, Oracle's access management, and Oracle enterprise gateway.
- Prevention against Insider Attacks: The proposed protocol registers the users using the Authentication server over a secure channel. Further, this offers protection against the stolen passwords. Thus, the proposed protocol resists insider attacks.
- Prevention against Forgery Attacks: A legal user of the system can launch a forgery attack against the eavesdropping and masquerading. To prevent Forgery, the hybrid management layer plays a vital authentication mechanism. The login message is encrypted with the help of a smart card. Therefore, the eavesdropper is unable to detect login request credentials.
- Secure Authentication: After receiving the login request message through the nearest user, the hybrid management layer verifies the user credentials and validates the authentication procedures.
- Mutual authentication: Mutual authentication is an essential feature for the verification of logistic services that are resistant to server spoofing attacks. First, the hybrid management layer checks authentication once the login request is sent. After successful authentication at the hybrid management layer, the user checks the authentication by decrypting the message from the business layer.
- Installation and Maintenance of Firewall: Firewall is an essential part of cloud computing for security purposes. Firewall installation and maintenance are required to ensure protection. All external devices must have a firewall interface. Firewall Policy and Rule Set Evaluation of routers should be reconfigured regularly. Create and Implement a Firewall that Denies Untrusted Access Source or application and records these events correctly. Create and implement a firewall to limit access to the system to direct external connections and those containing sensitive data or configuration data.
- Infected Applications: Firewall Cloud Computing service provider should have full access to the server, all rights for monitoring and management purposes of server maintenance. So this will prevent any malicious user from uploading any infected application, which can seriously affect other applications of the system.

The most prominent risk for mobile access to data in the cloud is authentication and authorization. Nowadays, 76% mobile applications operated with usernames and passwords, and these data are saved locally which leads to risks. Moreover, many passwords are stored in plain text; a hacker can crack a mobile device in a short period. Various solutions like Oracle provides authorization and authentication based approaches for mobile applications.

VI. CONCLUSION

Cloud-based logistics management helps business organizations to support flexible and reliable handling of a large amount of data. The article discussed unmentioned and undiscovered security issues that positively affect cloud systems. Recently, a wide range of researchers emphasized the known problems of the cloud systems and suggest various solutions. However, if a cloud system is to be widely adopted, better solutions are still needed. In this article, a conceptualized robust security framework for cloud-based logistics services is presented.

Moreover, a security enhancement layer is included at each layer of the cloud with a feasibility study on protecting user information in the logistics services ambiance. Also, the Data Residency for cloud-based logistics services is elaborated with Data Security analysis. Further, the article discusses the possible solutions to handle the security concerns of the logistic model. In the future, the cloud-based security through misbehavior detections and vulnerabilities assessment will be focused.

REFERENCES

1. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A., (2011). Cloud computing: The business perspective. Decision support systems, 51(1), pp.176-189.
2. Xu, X., (2012). From cloud computing to cloud manufacturing. Robotics and computer-integrated manufacturing, 28(1), pp.75-86.
3. Singh, A., Mishra, N., Ali, S.I., Shukla, N., and Shankar, R., (2015). Cloud computing technology: reducing carbon footprint in beef supply chain. International Journal of Production Economics, 164, pp.462-471.
4. Joosen, W., Lagaisse, B., Truyen, E. and Handekyn, K., (2012). Towards application driven security dashboards in future middleware. Journal of Internet Services and Applications, 3(1), pp.107-115.
5. http://www.manufacturing.net/articles/2012/03/the-rise-of-cloud-computing-extends-to-plm [Accessed 18 Jun. 2016].
6. Sharma V, Srinivasan K, Jayakody DN, Rana O, Kumar R. Managing Service-Heterogeneity using Osmotic Computing. arXiv preprint arXiv:1704.04213. 2017 Apr 13.
7. Sharma V, YouI, Jayakody DN, Atiquzzaman M. Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2017.12.039, 2017 Dec 28.
8. Cloud Computing Competence Center for Security, (2015). What are Deployment Models in Cloud Computing? [online] Available at: http://www.cloud-competence-center.com/understanding/cloud-computingdeployment- models/ [Accessed 18 Jun. 2016].
9. Rochwerger, B., Breitgand, D., Levy, E., Galis, A., Nagin, K., Llorente, I.M., Montero, R., Wolfsthal, Y., Elmroth, E., Caceres, J. and Ben-Yehuda, M., (2009). The reservoir model and architecture for open federated cloud computing. IBM Journal of Research and Development, 53(4), pp.4-1.
10. Sultan, N., (2010). Cloud computing for education: A new dawn?. International Journal of Information Management, 30(2), pp.109-116.
11. Alnashar, H.S., Elfattah, M.A., Mosbah, M.M. and Hassanien, A.E., (2015). Cloud Computing Framework for Solving Virtual College Educations: A Case of Egyptian Virtual University. In Information Systems Design and Intelligent Applications (pp. 395-407). Springer India
12. Harvard Business Review, (2010). Developing Competitive Advantage in the Cloud: Qualitative Findings. [online] Available at: https://hbr.org/2010/12/developing-competitive-advanta [Accessed 18 Jun. 2016].

13. Ke Xing, Wei Qian, Atiq Uz Zaman, Development of a cloud-based platform for footprint assessment in green supply chain management, Journal of Cleaner Production, Volume 139, 2016, Pages 191-203, ISSN 0959-6526, https://doi.org/10.1016/j.jclepro.2016.08.042.
14. David Villegas, Norman Bobroff, Ivan Rodero, Javier Delgado, Yanbin Liu, Aditya Devarakonda, Liana Fong, S. Masoud Sadjadi, Manish Parashar, Cloud federation in a layered service model, Journal of Computer and System Sciences, Volume 78, Issue 5, 2012, Pages 1330-1344, ISSN 0022-0000, https://doi.org/10.1016/j.jcss.2011.12.017
15. M. Fazio, A. Celesti, M. Villari and A. Puliafito, "How to Enhance Cloud Architectures to Enable Cross-Federation: Towards Interoperable Storage Providers," *2015 IEEE International Conference on Cloud Engineering*, Tempe, AZ, 2015, pp. 480-486. doi: 10.1109/IC2E.2015.80
16. X. Wang, "Analysis on Cloud Computing-based Logistics Information Network Mode," *2011 Seventh International Conference on Computational Intelligence and Security*, Hainan, 2011, pp. 1286-1289. doi: 10.1109/CIS.2011.285
17. A. Leinwand, The hidden cost of the cloud: Bandwidth charges, July 2009.
18. J. Gray, "Distributed computing economics," ACM Queue, vol. 6, pp. 63-68, May 2008.
19. Ramgovind S., Eloff M. M., Smith E., “The Management of Security in Cloud Computing” In PROC 2010 IEEE Interna- tional Conference on Cloud Computing 2010.
20. Srinivasan, K., Gupta, T., Agarwal, P. and Nema, A., 2018, April. A robust security framework for cloud-based logistics services. In 2018 IEEE International Conference on Applied System Invention (ICASI) (pp. 162-165).
21. Gupta, T., Choudhary, G. and Sharma, V., 2018. A Survey on the Security of Pervasive Online Social Networks (POSNs). arXiv preprint arXiv:1806.07526.
22. You I, Kwon S, Choudhary G, Sharma V, Seo JT. An Enhanced LoRaWAN Security Protocol for Privacy Preservation in IoT with a Case Study on a Smart Factory-Enabled Parking System. Sensors (Basel, Switzerland). 2018 Jun 8;18(6).
23. Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R. and Priyan, M.K., 2018. Centralized fog computing security platform for IoT and cloud in healthcare system. In Exploring the convergence of big data and the internet of things (pp. 141-154). IGI Global.
24. Sharma, V., Kim, J., Kwon, S., You, I., Lee, K. and Yim, K., 2018. A framework for mitigating zero-day attacks in IoT. arXiv preprint arXiv:1804.05549.
25. Sharma, V., Lee, K., Kwon, S., Kim, J., Park, H., Yim, K. and Lee, S.Y., 2017. A consensus framework for reliability and mitigation of zero-day attacks in iot. Security and Communication Networks, 2017.
26. Nuseibeh, B., Bandara, A., Khan, K.M., Khan, N.H., Nhlabatsi, A., Tun, T.T. and Yu, Y., QATAR UNIVERSITY, 2018. Method and system for adaptive security in cloud-based services. U.S. Patent Application 15/785,858.
27. Shin, D., Sharma, V., Kim, J., Kwon, S. and You, I., 2017. Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks. IEEE Access, 5, pp.11100-11117.
28. Win, T.Y., Tianfield, H. and Mair, Q., 2018. Big data based security analytics for protecting virtualized infrastructures in cloud computing. IEEE Transactions on Big Data, 4(1), pp.11-25.
29. Rao, B.T. and Anandam, D., 2018. A Novel Big Data based Security Analytics approach to detecting advanced attacks in Cloud Computing. International Journal of Research, 5(17), pp.517-523.
30. Dai, H., Ren, H., Chen, Z., Yang, G. and Yi, X., 2018. Privacy-Preserving Sorting Algorithms Based on Logistic Map for Clouds. In Proceedings of the 4th International Conference on Cloud Computing and Security (ICCCS 2018).
31. Uchenna CP, Nwankwo Wilson OB, Comfort O. Cloud-Based Virtual Organization Framework for Optimizing Corporate Value Chain. International Journal of Discrete Mathematics. 2018 May 4; 3(1):11.
32. Mushtaq MO, Shahzad F, Tariq MO, Riaz M, Majeed B. An efficient framework for information security in cloud computing using auditing algorithm shell (AAS). arXiv preprint arXiv:1702.07140. 2017 Feb 23.
33. Ukil A, Jana D, De Sarkar A. A security framework in cloud computing infrastructure. International Journal of Network Security & Its Applications. 2013 Sep 1; 5(5):11.
34. Tawalbeh L, Al-Qassas RS, Darwazeh NS, Jararweh Y, AlDosari F. Secure and efficient cloud computing framework. InCloud and Autonomic Computing (ICCAC), 2015 International Conference on 2015 Sep 21 (pp. 291-295). IEEE.
35. Arjunan K, Modi CN. An enhanced intrusion detection framework for securing network layer of cloud computing. InAsia Security and Privacy (ISEASP), 2017 ISEA 2017 Jan 29 (pp. 1-10). IEEE.
36. Marwan M, Kartit A, Ouahmane H. Design a Secure Framework for Cloud-Based Medical Image Storage. InProceedings of the 2nd international Conference on Big Data, Cloud and Applications 2017 Mar 29 (p. 7). ACM.
37. Al-Bahadili H, Al-Sabbah A, Abu Arqoub M. Modeling and Analysis of Cloud Collaborative Commerce. International Journal on Cloud Computing: Services and Architecture. 2013 Feb;3(1).
38. Tawalbeh LA, Ababneh F, Jararweh Y, AlDosari F. Trust delegation-based secure mobile cloud computing framework. International Journal of Information and Computer Security. 2017;9(1-2):36-48.
39. Bhagat BC, inventor; Bhagat Bhavesh C, assignee. Cloud computing governance, cyber security, risk, and compliance business rules system and method. United States patent application US 13/016,999. 2012 Jan 12.
40. Farrell R. Securing the cloud—Governance, risk, and compliance issues reign supreme. Information Security Journal: A Global Perspective. 2010 Nov 23;19(6):310-9.
41. Herland M, Khoshgoftaar TM, Bauder RA. Big Data fraud detection using multiple medicare data sources. Journal of Big Data. 2018 Dec 1;5(1):29.
42. Doshi N, inventor; Palo Alto Networks Inc, assignee. Single sign on proxy for regulating access to a cloud service. United States patent application US 15/792,033. 2018 Feb 15.
43. Qiu M, Gai K, Thuraisingham B, Tao L, Zhao H. Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. Future Generation Computer Systems. 2018 Mar 1;80:421-9.
44. Liu L, De Vel O, Han QL, Zhang J, Xiang Y. Detecting and Preventing Cyber Insider Threats: A Survey. IEEE Communications Surveys & Tutorials. 2018 Jan 1;20(2):1397-417.
45. Mittal V, Gupta S, Choudhury T. Comparative analysis of authentication and access control protocols against malicious attacks in wireless sensor networks. InSmart Computing and Informatics 2018 (pp. 255-262). Springer, Singapore.
46. Scheffler S, Smith S, Gilad Y, Goldberg S. The Unintended Consequences of Email Spam Prevention. InInternational Conference on Passive and Active Network Measurement 2018 Mar 26 (pp. 158-169). Springer, Cham.
47. Sharma V, Guan J, Kim J, Kwon S, You I, Palmieri F, Collotta M. MIH-SPFP: MIH-based secure cross-layer handover protocol for Fast Proxy Mobile IPv6-IoT networks. Journal of Network and Computer Applications. 2019 Jan 1;125:67-81.
48. Chamberlain RD, Chambers M, Greenwalt D, Steinbrueck B, Steinbrueck T. Devices Can Be Secure and Easy to Install on the Internet of Things. InIntegration, Interconnection, and Interoperability of IoT Systems 2018 (pp. 59-76). Springer, Cham.
49. Kharchenko V, Kolisnyk M, Piskachova I. The research of the smart office availability model considering patches on the router firewall software. In2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) 2018 May 24 (pp. 169-174). IEEE.
50. Miao Y, Ruan Z, Pan L, Wang Y, Zhang J, Xiang Y. Automated Big Traffic Analytics for Cyber Security. arXiv preprint arXiv:1804.09023. 2018 Apr 24.
51. Helmi AM, Farhan MS, Nasr MM. A framework for integrating geospatial information systems and hybrid cloud computing. Computers & Electrical Engineering. 2018 Apr 30;67:145-58.
52. Singh A, Chatterjee K. Cloud security issues and challenges: A survey. Journal of Network and Computer Applications. 2017 Feb 1;79:88-115.

AUTHORS PROFILE

Kathiravan Srinivasan is the Professor (Associate) of Machine Learning and Artificial Intelligence in the School of Information Technology and Engineering at Vellore Institute of Technology (VIT), Vellore, Tamil Nadu, India. He was previously working as a Faculty/Lecturer in the Department of Computer Science and Information Engineering and also as the Deputy Director- Office of International Affairs at National Ilan University, Taiwan. He has around 15 years of research experience in the area of Machine Learning, Artificial Intelligence, and its Applications.

He received his Ph.D., in Information and Communication Engineering, M.E., in Communication Systems Engineering and B.E., in Electronics and Communication Engineering from Anna University, Chennai, India. He has won the Best Conference Paper Award at 2018 IEEE International Conference on Applied System Innovation, Chiba, Tokyo, April 13-17, 2018.

Moreover, he has also received the Best Service Award, Department of Computer Science & Information Engineering, National Ilan University, Taiwan. In 2017, he won Best Paper Award at 2017 IEEE International Conference on Applied System Innovation, Sapporo, Japan, May 13-17, 2017 and Best Paper Award at International Conference on Communication, Management and Information Technology (ICCMIT 2017), Warsaw, Poland. In 2016, he received the Best Service Award as the Deputy Director at the Office of International Affairs, National Ilan University. He is presently serving as the Editorial Board member and Editor of IEEE Future Directions and KSII Transactions on Internet and Information Systems (TIIS), Associate Editor for IEEE Access, IET Networks and Journal of Internet Technology, and Editorial Board Member and reviewer for various IEEE Transactions, SCI, SCIE and Scopus Indexed Journals. He is the guest editor MDPI Future Internet, Journal of Mobile Multimedia, International Journal of Distributed Sensor Networks and Recent Patents on Computer Science. He has played an active role in organizing several International Conferences, Seminars, and Lectures. He is an IEEE Senior Member and has been a keynote speaker in many International Conferences and IEEE events. His research interests include Machine Learning, Artificial Intelligence, Deep learning, Communication Systems & Networks, Multimedia, and Data Analytics.

Takshi Gupta received the B.Tech. degree in Computer Science and Engineering from Punjab Technical University in 2012 and the PG Diploma in Business Administration from SCDL, Symbiosis University, India in 2014 both with distinction. She is currently associated with the MobiSec Lab, Department of Information Security Engineering, Soonchunhyang University, Asan, South Korea. Prior to this, she worked at Kochar InfoTech followed by Gen-XT Infosystems and was a co-founder at Future Info-Systems. In 2017, she won a Best Paper Award at IEEE International Conference on Applied System Innovation, Sapporo, Japan, May 13-17, 2017. Her areas of research and interests are database management and security, artificial intelligence, and semantic webs.

Senthil Kumaran S is currently working as Associate Professor, Department of Mechanical Engineering, Vellore Institute of Technology-VIT University, Vellore, Tamil Nadu, India. He has been working for more than 10 years in various Engineering Institutions. He has guided various under-graduate, post-graduate students and 3 Ph.D. research scholars supervised in the field of quality improvement of the process in a different field such as friction welding, Tribology, Non-Traditional Machining Process, and composite materials.

He has completed his research work in Friction welding process improvement at the National Institute of Technology, Tiruchirappalli, and Tamil Nadu. His research interests in Advance solid-state welding process, Materials and Metallurgy, Composite materials and Quality Management, Unconventional machining process, Optimization, Material characterization and Mechanical Behavior of Material. He has published more than 125 'Internationals' reputed Journals and conferences. His contribution to the research work such as Genetic Algorithm, Acoustic Emission, Artificial Neural networks, fuzzy logic and optimization techniques in quality improvement of Manufacturing Process, etc.

He received Young Scientist Award from Department of Science and Technology (DST), Science and Engineering Research Board (SERB), New Delhi in the year 2014 and he has completed a research project in the year 2017 under the topic of friction welding of SA 213 tube to SA 387 tube plate using an external tool. Also, he received an outstanding reviewer award and recognized reviewer award from Elsevier journals. He was a lifetime member of Indian Society of Technical Education (ISTE), Indian Welding Society (IWS), International Association of Engineers (IAEng) and International Research Engineers and Doctors (IRED). Also, looking forward to guiding many research scholars, often developing his own interests in the field which he was expertised.

Srinivasan Narayanan is currently working as an Assistant Professor (senior) at the Department of Mechanical Engineering in the Vellore Institute of Technology-VIT University, Vellore, Tamilnadu India. He has completed institute post-doctoral studies at IIT Madras (Chennai India), and Ph.D. in IIT Bombay (Powai India) and Monash University (Melbourne Australia). He has guided various under-graduate, post-graduate students. His research work includes metallurgy, plastic deformation, corrosion, and quality engineering. He has published lot of international journal articles of high repute and participated international conferences.