Chapter - 2

LITERATURE SURVEY
CHAPTER - 2

LITERATURE SURVEY

2.1 INTRODUCTION

This chapter surveys the existing techniques and frameworks that are related to the cloud computing attacks, security and quality of services (QoS). Moreover, the advantages and disadvantages of each and every method are investigated in this chapter. The cloud computing has some security issues, such as, loss of control, lack of trust and the multi-tenancy. The attacks mainly occur in the storage capacities of cloud network, processing power but cloud provides high quality service and limited resources. Side Channel Attack (SCA) includes Simple Power Analysis (SPA), Differential Power Analysis (DPA), Correlation Power Analysis (CPA), Mutual Information Analysis (MIA), and Algebraic Side Channel Collision Attack (ASCCA). These attacks of physical leakages are compared with the actual measurement. Cryptographic algorithms provide security against rival which is the black box access to the cryptographic devices. The SCA is developed with the possibility to exploit the physical leakages such as, power consumption or electromagnetic radiation.

2.2 CLOUD COMPUTING IN QOS

Wu et al. (2013) [59] proposed the scheduling algorithm based on the QoS-driven in cloud computing. The special attributes of task and the sorts tasks are computed by their priority. The different services of each task were evaluated by the algorithm. The scheduling was used to complete the task faster. The result had the
good performance and load balancing in QOS driven from both priority and completion time. The QoS scheduling was classified as the task based on low priority and high priority. The result was analyzed by the user privilege, expectation, task length and the pending time in queue and throughput. Minimum computation time was used in each task. The advantage of the algorithm was to reduce the computation time.

Abdullah and Othman (2013) [2] reviewed the use of Divisible Load Theory (DLT) to design efficient strategies to minimize the processing time in scheduling. The DLT was used to minimize the total cost. It was used to design and analyze the problem of the scheduling jobs. Rigorous simulation environment was used for analyzing. It considered the real-time job allocation restriction, such as, political concern and machine failure. Optimization was used to reduce the problem of scheduling. The system was integrated with the cloud infrastructure to improve their performance.

Mukhopadhyay et al. (2013) [38] developed effective Web Services Cloud Computing in QOS framework. The required web services used nonfunctional attributes of web services in service consumers. The nonfunctional attributes possessed reliability, availability, response time and latency. The service discovery query was a part of QoS requirement to provide service to the consumer.

2.2.1 Issues in current clouds

- Lack of technicality
- Need of effective initial investment
- Privacy maintenance
The QoS is applied with web service discovery in registration, verification, certification and confirmation. The service negotiation and service composition were based on the QoS based cloud service discovery. An appropriate service from the log of service available was found in the discovery process. Service Name Matching Block (SNMB) was responsible for similarity, compatibility and numerical reasoning. Web service cloud computing work in two ways - uniqueness and consequence. These two ways were applied in the service matching, service rank, and service filtering.

Das et al. (2013) [12] developed an adaptive QoS-aware VM provisioning mechanism used for the system resources. The network model included admission control, resource manager, VM server, input ques. The cloud contained three layers, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a service (SaaS). QoS-Aware Adaptive VM Recycling and provisioning approach were presented by the automated, flexible and efficient management of cloud resources. The performance was analyzed by the simulation time and a number of rejection requests. The cloud computing is a multiple application but still, it contains some obstacles and complexities. An intelligent approach to VM and QoS provisioning system were used to remove some complexities. The algorithm was used to minimize the rejection rate in cloud data centers. The benefits of the mechanism created jobs in the queue. Creation of VM is only for the time critical jobs. The VM server determined the jobs in critical time.

Aazam et al. (2014) [1] presented a stochastic model to evaluate the performance of the IaaS cloud system. The cloud infrastructure was required to predict and quantify the cost benefit of a strategy. An analytical model, based on the
Stochastic Reward Nets (SRNs) which are both scalable to model systems were composed of the thousands of resources and flexible to represent different policies and cloud strategies. The different performance analysis of the data center was analyzed, such as utilization, availability, waiting time and responsiveness. Account load bursts were provided in the resiliency analysis. Cloud was used to measure the accurate QoS. The quality of service, cloud service provisioning of Service Level Agreements (SLA) were required in the business requirement. The complexity was analyzed in the requirement of the scalability.

Salot (2013) [46] analyzed various scheduling algorithm in a cloud environment. The task scheduling consumed more communication cost. The scheduling played a major role in cloud computing. More algorithms are used in the scheduling process. The scheduling algorithms were not able to provide the scheduling in the cloud environment. In cloud computing, scheduling was classified into two, such as,

- Batch Mode Heuristic scheduling Algorithm (BMHA)
- Online Mode Heuristic Algorithm (OMHA)

The batch mode heuristic algorithm was classified as,

- First Come First Served Scheduling Algorithm (FCFS)
- Round Robin Scheduling Algorithm (RR)
- Min-Min algorithm
- Max-min algorithm
The Most Fit Task scheduling algorithm (MFT) was mostly used in the online mode heuristic scheduling algorithm. The scheduling process in cloud computing was classified as three stages namely,

- Resource discovering and filtering
- Resource selection
- Task submission

The scheduling algorithm provided high throughput, and cost-effective but it does not consider reliability and availability. The demerit of the algorithm was to improve the availability and reliability in the cloud.

Zheng et al. (2013) [69] evaluated the quality of service ranking prediction frame work for cloud services. For making the optimal cloud service, the Quality of System (QoS) ranking provided the valuable information. QoS ranking avoided time consumption and service invocation. QoS ranking prediction performances were compared with nine methods, such as,

- User based collaborative filtering method using Vector Similarity (UVS)
- Item based collaborative filtering method using Vector Similarity (IVS)
- User based and Item collaborative filtering using Vector Similarity (UIVS)
- User based collaborative filtering method using Pearson Correlation Coefficient (UPCC)
- Item based collaborative filtering method using Pearson Correlation Coefficient (IPCC)
- User based and Item based collaborative filtering using Pearson Correlation Coefficient (UIPCC)
- Greedy
- Cloud Rank 1
- Cloud Rank 2

In making QoS ranking, no additional service invocations were required in the cloud services of QoS ranking prediction framework. The ranking approach was identified and aggregates the performance between the pair of service to produce a ranking of services. The output was compared with the rating based approaches and traditional greedy method.

LD and Krishna (2013) [29] designed the honey bee behavior inspired load balancing (HBB-LB) to achieve balanced load across the virtual machines for maximizing the throughput. The honey bee foraging behavior was a combination of the both Artificial Bee Colony (ABC) and an optimization algorithm. Numerical function optimization was presented in the algorithm. Neighborhood source production mechanism was implemented in the ABC algorithm. In digital signal processing, leaf constrained minimum spanning tree problem, flow shop scheduling problem and block matching algorithm were used in the ABC algorithm. HBB-LB
algorithm used two policies such as, First In First Out (FIFO) and Weighted Round Robin (WRR). Performance was analyzed in terms of response time of virtual machine in HBB-LB, Dynamic Load Balancing (DLB), and WRR. The quality of services required security, cost, and speed. The HBB-LB algorithm performed better than DLB and HDLB algorithms and also provided the more efficiency with less number of task migration compared with DLB and Honey Dynamic Load Balancing (HDLB) techniques.

Papagianni et al. (2013) [41] developed the approximation approach to address the problem in substrate resources. The efficiency of the system was flexible, structured and comparative performances. Mixed Integer Programming (MIP) problem was as cloud mapping problem in the optimal network. Controlling Virtual Infrastructure (CVI-Sim) implemented in the simulator is called a discrete event java based simulator. Graph was drawn between the manipulation, analysis, and visualization of the data. The JFC framework was implemented in the graphical user interface simulator. The Networked Cloud Mapping (NCM) approach had demerits, such as,

- Greedy Node Mapping (GNM) - shortest path algorithm for link mapping phase
- Multi Commodity Flow (MCF) problem was solved by the greedy node mapping.
The performance was evaluated by acceptance ratio, hop count, mapping revenue and mapping cost. Reconfiguration policies may vary depending on several operational parameters such as,

- The degree of utilization of substrate resources
- Unbalanced allocation of substrate resources
- Service prioritization policies

A polynomial time solution was lead to the application of randomized rounding technique. The Link mapping was used to solve multi-commodity flow problems. An appropriate reconfiguration strategy was adopted with a highly dynamic networked cloud environment.

Lin et al. (2013) [31] established the QoS Aware Data Replication (QADR) algorithm in cloud computing. It was consisted of two algorithms namely,

- High QoS First Replication (HQFR) algorithm
- Minimum Cost Maximum Flow (MCMF) algorithm

The first algorithm agreed on data replication and greedy algorithm did not minimize the data replication cost and the number of QoS violated data replicas. The second algorithm transformed the QoS Aware Data Replication (QADR) in polynomial time, but it took more computational time. The advantage of the algorithm was data replication and recovery. The QADR problem was obtained by integer linear programming (Sood and Bansal) formulation. The QADR problem was transformed to a Minimum Cost Maximum Flow (MCMF) problem. This method included an
algorithm of high QoS first replication algorithm. The advantage of the C_MCMFR algorithm reduced the computation time of the QADR problem. It was solved by reduced execution time. The Hadoop and random algorithm took less time. The QoS Aware Data Replication (QADR) problem was solved by additional requirements of applications. The optimal solution was not achieved by the greedy algorithm to solve the QADR problem. In the greedy algorithm, the data replication cost and the number of QoS-aware data replicas cannot be minimized. The simulation result was showed that the replication algorithm efficiently performed the QoS-aware data replication in the cloud computing systems. The disadvantage of the algorithm was less energy consumption.

Garg et al. (2013) [21] Suggested Cloud Service Measurement Index Consortium (CSMIC) framework based on common characteristics of the cloud services. Several enterprises including amazon, google, IBM, Microsoft were started to offer different cloud services to their customers. The mechanism and framework were used to measure the quality and prioritize cloud services. The Service Level Agreement (SLA) was used to improve their QoS. Service Measurement Index (SMI) was designed based on the International Organization for Standardization (ISO) standards of Cloud Service Measurement Index consortium (CSMIC). The SMI has the following characteristics, such as accountability, agility, cost, performance, assurance, usability, security, and privacy. The efficiency of the service availability was measured by the response time. The service response time depended on the sub factors, such as average response time, and maximum response time. The merits of the cloud Key Performance Indicator (KPI) were,
Sustainability : It was measured by the energy efficiency of the cloud services

Suitability : The customer requirements were met at the cloud provider

Accuracy : It is compared with the expected values

Transparency : It was considered as important features of the cloud provider

Usability : The cloud service was defined by the attributes of the usability.

The components of usability were operability, learn ability, and install ability and understandability.

Interoperability: The ability of the service to interact with other services or the same services.

Availability : The service access time of customer in percentage

Reliability : Service operators without failure of given time and condition

Stability : It was defined as the variability in the performance of the service

Adaptability : To adjust changes in the service, based on customer request was provided by the service provider.

Elasticity : It was defined as the cloud service scaled during the peak times.

Throughput and Efficiency : It was the important measurement to evaluate the performance of the infrastructure service provided by the clouds.

The cloud services based on the different application evaluated the Analytical Hierarchical Process (AHP) based on ranking mechanism. The cloud provider
provided different cloud services with different price and the performance attributes. Performance and security were the parameters of the cloud service requirements.

Dong et al. (2013) [13] introduced the QoS oriented cloud computing resources availability. The monitoring model of the cloud computing resources availability was created by the dynamic process of the cloud computing. The QoS of cloud resources were connected by some model to provide the services, such as series model, parallel model, and mix model. The common attribution and single cloud attribution were used to analyze the availability of the cloud computing resources. Three models were used to monitor the cloud computing services. Different cloud services were provided the different services. There were multiple attributes about the quality of the services. The cloud computing resources were calculated by the weight of different attributes and depend on the services. The local optimization algorithm used in the mathematical model was designed to solve the resource selection problem. The optimal model algorithm was a failure in the overall demand of the customer in the cloud services.

2.3 SECURITY IN CLOUD COMPUTING

Singh (2014) [51] reviewed the security in cloud computing, it was totally internet dependent technology where the data was stored and maintained the data center of a cloud provider. The cloud computing model came from grid computing, distributed computing, parallel computing, and virtualization technology. The data privacy and the service availability in cloud computing were the keys of security problem. The cloud computing architecture contained services layer, access layer, user layer and the cross layer. It included security, management, and privacy. The Platform as a Service (PaaS), the Internet as a Service (IaaS) and the Software as a Service (SaaS) were the services provided by the cloud. This model was classified as
private cloud, public cloud, community cloud and hybrid cloud. The trust of the cloud service user contained responsibility ambiguity, loss of governance, loss of trust, service provider lock-in, secure cloud service user access, lack of information or management, data loss and data leakages. The threats of the cloud service providers included responsibility ambiguity, production inconsistency, evoluntional risks, and business discontinuity, and supplier lock-in, license risks. The cloud contained some security problems, such as virtual machine security, network security, data security, privacy, integrity, location, and availability. The cloud service providers were required to inform their customers on the level of the security and provided by the cloud. Security was the main problem in cloud computing. Network and virtualization were the other security challenges in the cloud.

Pancholi and Patel (2016) [40] developed AES algorithm for secure data storage in cloud computing. The cloud computing model combined the SaaS, PaaS and IaaS. These achieved the business goal with minimum effort compared by the traditional computing environment. The cryptography method was important in secure cloud computing. It was provided the symmetric and asymmetric algorithm for secure data. The AES was termed as symmetric cryptographic algorithm. The cryptographic algorithm was grouped with three algorithms, such as symmetric key algorithm, asymmetric key algorithm and the hash function. The symmetric key algorithm was used for the same key for both encryption and decryption process. Asymmetric key algorithm used different key for encryption and decryption process. The hash function used the message or secure hash function used the encryption and decryption process. The AES algorithm contained four functions such as sub byte, shift row, mix column and add round key. AES algorithm was easy to implement and it was faster to provide flexibility and scalability. AES algorithm required less memory compared to blow fish algorithm. AES algorithm provided security because it used 128,192 or 256-bit keys.
Shahzad (2014) [48] surveyed cloud computing security and their approaches and solutions as shown in Figure 2.1.

![Cloud Computing Model Diagram]

**Figure 2.1 Cloud Computing Model**

Resource pooling and rapid elasticity were the characteristics of cloud computing. Security in the cloud was an important measurement. Security and privacy were the major hurdles of cloud computing. The uniqueness of the cloud environment includes outsourcing, extensibility and shared responsibility, virtualization, multi-tenancy, service level agreement and heterogeneity. The Amazon web services provided security in the following ways, such as certification and accreditations, physical security, secure services and data privacy. The Amazon EC2 instance was protected by one or multiple security groups, termed as, set of rules that
specify the ingress network traffic. The user identified TCP, UDP ports, and source codes. The firewall protection of running instances provided the security for their groups.

The Cloud Computing has the five essential characteristics of cloud computing, at several locations for either redundancy or fault tolerance. Security measure was adopted by the largest cloud service provider with their infrastructure security.

Hussain et al. (2016) [25] presented the security attacks of each layer in the cloud. The threats were generally found in the privacy breach, data leakage, and unauthorized data access at different cloud layers. The attack types and risk level was associated with different cloud services. The Risk was classified as, low, medium and high. The position of cloud layers depended on the intensity risk level. The intensity of risk included security requirements, such as data encryption, multi-tenancy, data privacy, authentication and authorization of different cloud services. Dynamic security contract is used for each cloud layer. The security of cloud computing was classified into three, such as SaaS, PaaS, Iaas. Software as a Service (SaaS) was exposed to the attack of API publishers. The attacks were affected by data privacy. They were contained two tools, such as,

- Attacks on development tool
- Attacks on management tool

The web portals were mainly affected by unauthorized access and data privacy. The intruders were trying to extract the sensitive information of API keys and private keys. The attack layer was as exposure of secure shell for extracting key
credentials. Data protection, attacks on the interfaces and attacks on the Secure SHell (SSH) were present in the SaaS.

2.3.1 Data protection

In cloud computing, data privacy was important in shared resource environments. It had three major challenges, such as integrity, authorized access, and availability. Data integrity was used for the data which was not corrupted or tempered during the communication. The data was shared or communicated between the common network bones. Authorized access prevented the data from the intrusion attacks. Malicious attackers or the intruders have hidden the proxy application between the cloud provider and the information of the login credentials.

Attacks on interfaces: Cloud interfaces were the root level access to the machine without direct attack on the cloud interfaces. An authentication mechanism was classified into two, such as,

- Control interfaces vulnerable to signature wrapping
- Advanced cross Site Scripting (XSS) technique

The attack was referred by signature wrapping attack. Username and the password pair information was sealed by particular vulnerability attacks.

Attacks on Secure Shall (SSH): The attacks on the secure shall be used to establish the trust and connection with the cloud server. The attacks on API keys, attacks on user credentials and the attacks on the publisher credentials were included in the different types of attacks on SSH.
Security concern with the infrastructure as a service and the platform as a service: The IaaS and PaaS were overlapped in the model due to their interdependency on each other. The attacks on these layers were grouped, such as,

- Attacks on cloud services
- Attacks on virtualization

The Service Level Attack (SLA) was combined with the Web Service Level Agreement (WSLA) for the security risk. The Dynamic Security Contract (DSC) between cloud consumer and a provider was implemented across the layer according to the requirements of services and security. The level of severity of the attack was assessed as too low, medium and high. Security requirements included data encryption, data privacy, multi-tenancy, authentication, and authorization.

Nafi et al. (2013) [39] proposed a new security structure for cloud computing environment based on file encryption and distributed data. It includes AES file encryption system, RSA system for secure communication and one-time password to authenticate the user and MD5 hashing for hiding information. In private cloud system, the information was shared only in the cloud. An asynchronous key system and AES based file encryption system for exchanging the information or data was included in the model. The security algorithms work with,

- RSA algorithm for secured communication
- AES for secured file encryption
- MD5 hashing for covering the tables from user
- One time password for authentication

For security communication, the RSA encryption algorithm was used. It used system public key for encryption process. The algorithm contained private key for decryption process. These were used for secure communication. The one time
password was used for authenticating process. It used user login for security communication. In this communication, the authentication user only knows the username and password. Password was generated randomly and each time the user creates a new password. The new password was updated for the particular user and the old password was erased automatically. This model was ensured with security for cloud computing structure. The execution time was not high because each algorithm was done on different servers. The information and uploaded files were not easily received because they need control over the servers which was a difficult one. The encryption algorithm was used in secure communication.

Figure 2.2 Eco Systems of Cloud Security and Privacy
Ahmed and Hossain (2014) [3] reviewed the security issues in cloud computing as in Figure 2.2. Cloud computing contained three sensitive states in the operational context of cloud computing, such as,

- Transmission of data to the cloud
- Transmission of data from the cloud server to client’s computers
- Storage of client data in remote cloud servers.

In cloud computing infrastructure as a distinct layer was conceptualized in security. Security for cloud computing was a non-compromising requirement. The cloud computing was offered virtual ownership and access to the supercomputer without procuring physically. In cloud computing, the security issue was not related to technical and direct security breach. The cloud computing combined both technical and social setting. The cloud computing was analyzed with social, business, technical and legal perspective.

Zhao et al. (2014) [67] endorsed the Craig gentry construct homomorphism encryption scheme. It included four algorithms, such as key generation algorithm, encryption algorithm, decryption algorithm and additional evaluation algorithm. The fully homographic encryption was included two basic homomorphism types namely,

- Multiply homomorphic encryption algorithm
- Additively homomorphic encryption algorithm

Security infrastructure was required to safeguard web and cloud services. The user level needs to perform the trust negotiation and reputation aggregation of all users. The distributed DoS attack was needed to establish security precautions in the
worm containment and intrusion detection against virus, worm. Deploy mechanism was used to prevent online piracy and copyright violations of the digital count. The security responsibilities were divided between cloud providers and users differently for three cloud service models. The providers were totally responsible for platform availability. The confidentiality issues were responsible for IaaS user. The PaaS and SaaS services provided were equally responsible for preserving data integrity and confidentiality. The cloud security problem was faced by homomorphic encryption mechanism. It ensured transmission data between cloud and user safety.

Ali et al. (2015) [4] surveyed cloud computing security and their opportunities and challenges. Additional security threats were provided by the third party cloud service. Cloud computing architecture frameworks had the contained the following characteristics, such as,

- On demand self service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service
- Multi-tenancy

2.3.2 Service model

The service model was divided into three such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS did not provide the facility to create an application or software. PaaS was included in
Integrated Development Environment (IDE). The IaaS was referring to the hardware infrastructure provided by the CSP including network, storage, memory, processor and other computing resources. Cloud was also classified into four, such as private cloud, public cloud, community cloud and hybrid cloud. The cloud computing characteristics were measured by optimization and low-cost service to the customer. The communication between customer and cloud used standard internet protocol and their mechanisms. The cloud communication was classified into two, such as communication external to the cloud and communication internal to the cloud.

2.3.3 Shared communication infrastructure

It sanctioned the sharing of network infrastructure components but it was not sharing the computational and storage resources. The sharing network components provided the attackers, a window of cross tenant attack.

2.3.4 Virtual network

In cloud computing, the virtual network was used in communication. The virtualized network was able to generate the security of cloud environment.

Security misconfigurations: It provided secure cloud service to the user. It compromised the security of the customer, application and the system. Ten risks in the web application were identified in the open web application security, such as injection, broken authentication and session management, cross-site scripting, insecure direct object reference, security misconfiguration, sensitive data exposure, missing function level access control, cross-site request forgery, vulnerable components, invalidated redirects and forwards. The cloud computing needed security
against insider threats. Security solution provided advantages to the user and CSP. They also used the computational and cost overhead.

Modi et al. (2013) [37] surveyed the security issues and solution of different layers of cloud computing. The survey depended on the factors affecting cloud computing adoption, vulnerabilities, and attacks and identified the relevant solution directives to build security and privacy in cloud computing environment. The vulnerabilities, threats and attacks occurred as several security problems. A threat in the cloud was a potential event which was malicious or incidental. An attack was an action to harm cloud resources. The availability and productivity of cloud computing were affected by exploitation of vulnerabilities. Vulnerabilities in virtualization were basis for cloud computing architecture. Three types of virtualization were used, such as OS level virtualization, application based virtualization, and hypervisor-based virtualization. Cloud providers were increased to maintain the maximum level of isolation between Virtual Machine (VM) instances with isolation between inter-user processor. Operating system getting the read or write access to bypass the security mechanisms were Data Execution Prevention (DEP), safe Structured Error Handling (safeSEH) and Address Space Layout Randomization (ASLR). An implicit way of attacking cloud system included common types of attacks like man-in-the-middle attack, IP spoofing, ARP spoofing, DNS poisoning, RIP attacks and flooding. Then user managed their subscription with cloud instance, data upload or data computation via the management interface. The potential threats relevant to the cloud were changes to the business model, abusive use of cloud computing, insecure interfaces, API, malicious insiders, shared technology or multi-tenancy nature, data loss, and leakage, service hijacking, risk profiling, identity theft. Cloud computing comprised
of many attacks, such as zombie attack, service injection attack, virtualization attack, man-in-the-middle attack, meta spoofing attack, phishing attack, cross-site scripting, and backdoor channel attack. The attacks were affected directly or indirectly in terms of confidentiality, integrity, and availability of cloud resources. The security concerns are based on different levels via, application level, network level, data storage level, virtualization level, authentication and access control level. Attacks on data storage were directly affected by the security of user data with application data and sensitive data. Authentication and access control level risks affected the security of legitimate user services and resources. Auditing and regulation levels threats were directly affected by user data privacy, confidentiality, and integrity.

Mahajan and Sachdeva (2013) [35] surveyed three encryption techniques like AES, DES and RSA algorithm. This algorithm was the performance of encryption techniques based on the simulated time of both encryption and decryption. Data Encryption Standard (Zhou, et al.) algorithm provided a standard method for protecting sensitive commercial and classified data. Advanced Encryption Standards (AES) algorithm was not secure but the algorithm provided high speed. AES algorithm consumed least encryption and RSA consumed the longest encryption time. Decryption of AES algorithm was better than other DES and RSA algorithm.

Kaur and Singh (2013) [27] developed encryption algorithm for security of cloud computing. The cipher cloud framework kept their data confidentially on public cloud. The cipher cloud utilized two-step encryption process. The data was sent from client to the cloud server or the cloud server sent the data to the client. The public was not secured in the data transformation because all users accessed the data without
encryption and decryption process. The selective encryption technique provided data confidentiality. Computing resources and the data was maintained and provided by cloud services. The cloud security used the following algorithms,

- RSA algorithm
- DES algorithm
- AES algorithm
- Blowfish algorithm

The cipher cloud encrypted the data independent from the facts of data to be stored and the user has decrypted the data from the cloud by using the algorithms. The data was safe in the HTTPS TLS 1.0 standard transmission. Data was required for operational and management security controls. The hybrid cloud has depended on the gateway between the private and the public cloud.

Waizenegger et al. (2013) [58] developed the policy aware cloud service approach for enabling secure cloud computing. Some methods were used in the policy aware cloud service provisioning, such as enabling and configuring policies through offering, interfering policies, global and local policies. It described different layers in the service topology. The policy was effective for multiple nodes or relationships at a same time. The Topology and Orchestration Specification for Cloud Applications (TOSCA) were standardized by OASIS for cloud services. The multiple policies were combined with formal TOSCA cloud services. Two approaches were used in the cloud service life cycles, such as p-approach and the IA- approach. TOSCA was used to allow the node templates or node types for reusing different topologies.
Almorsy et al. (2016) [6] Surveyed the security problem in the cloud computing. Security problem was more complicated in cloud model. The problem was related to architecture, multi-tenancy, elasticity and layers dependency. The cloud service delivery models included Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and the Software as a Service (SaaS). Cloud computing has decreased the cost while increasing the resource utilization. Multi-tenancy and elasticity were two key characteristics of cloud computing model. Deep stack of dependent layer depended on the cloud computing model. The IaaS models covered cloud physical infrastructure layer, virtualization layer, and the virtualized resources layer. The PaaS layer covered platform layers, API, and services layer. The cloud computing model included cloud provider, service provider, and the service consumer.

Multi-tenancy and isolation were the major problems in cloud security. The security management was very critical to control. The holistic cloud security model
used model-based approaches to capture different security. The APIs provided flexible security interfaces. Support integration and coordination with the other security controls at different layers delivered integrated security. The multiple clouds integrated bigger pool of resources or integrated services and their security requirements were federated and enforced to different cloud platforms. The cloud computing enabled following federation, such as,

- Identity and Access Management (IAM) and federation
- Key management
- Security management
- Secure software development life cycle
- Security performance tradeoff optimization
- Federation of security among multicourse

Figure 2.4 Cloud Service Delivery Models
Sachdev and Bhansali (2013) [45] utilized AES algorithm for cloud computing security. The simple data protection model for data encryption is Advanced Encryption Standard (AES) as shown in Figure. 2.4. It provided data confidentiality and security. Cloud computing security had multi-tenancy, data loss and leakages, identity management, patch management and internal threats. The AES symmetric encryption algorithm with a key length of 128 was used to decide cloud service and migration, and the encryption process was done by AES algorithm. The encryption process works at different stages, such as sub bytes, shift rows, mix column, and add round key. An encryption process was compared with varies algorithms, such as AES, DES, and triple DES. Cloud service was increased for security problems. The cloud justified the security issues and satisfied the users. AES algorithm had consumed lesser memory and computational time. AES provided security from many attacks.

Tebaa and Hajji (2014) [55] utilized homomorphism encryption for secure cloud computing. The cloud provider provided the guarantees for protection of privacy and sensitive data stored in their data center. Different virtualization techniques were used in cloud computing security, such as virtual machine, isolator, full hypervisor, and Para virtualization. The characteristics of cloud computing services were, elasticity, ability to adapt, quality of service, high availability, cost reduction, and ecological approaches. The cloud computing lacked security, confidentiality, and visibility.

The cloud server does not guarantee better security and confidentiality of the customer data. The cloud provider performed operation of encrypted data without decrypting used in the cryptosystems based on homomorphism encryption. It
analyzed different encryption cryptosystems of cloud computing platform. The characteristics were compared with homomorphism encryption type, privacy of the data and security applied in the keys. The disadvantage was the cloud provider depended on size of the encrypted messages and length of the public key.

Yuan and Yu (2014) [65] proposed secure and practical multiparty BPN network learning scheme. It solved the problem by using power consumption of cloud computing. In this scheme each user has encrypted the data and uploaded the cipher text in the cloud. The scheme provided security, efficiency and accuracy. The algorithm allowed multiple parties to perform secure scalar products and homomorphism operations. The parties encrypted their arbitrary partitioned data and uploaded the cipher texts to the cloud. The BGN homomorphic encryption algorithm supported multiparty scenario, it used independent solution of related applications.

Dong et al. (2014) [14] presented privacy preserving and secure data sharing scheme in cloud computing. It achieved effective, scalable and flexible privacy preserving data policy with semantic security. The policy of cloud user and secure cloud computing was included in file creation, user revocation, and modification of user attributes. (The security analysis was securing the generic bilinear group model in the random oracle model). To improve the privacy and security for data sharing in cloud computing, Cipher Policy Attribute-Based Encryption (CPA-BE) and Identity-Based Encryption (Seibert, et al.) were used. The scheme introduced hash function that mapped user IDs to group the elements in the algorithm. The scheme integrated four algorithms such as system initialization, encryption, key generation and decryption. The user used the encryption algorithm to encrypt the files with the attributes and upload to the cloud. Flexibility and different access were privileges for each user to achieve fine-grained access control. The performance was measured by
number of attributes, communication cost, and revocation operations. The scheme had low overhead and highly efficient. The disadvantage was the privacy preserving and effective cloud data sharing service were not used in the real Cloud Service Provider (CSP) platform.

Yang et al. (2015) [62] utilized a combination of mixed storage system based on the combination of multimedia data with multimedia monitoring system. The multimedia protection was based on role access control. The complete process of the system was registration, role assignment, encryption, and decryption. It provided guarantee for security of data or files. The security was analyzed by resist known attacks, anti-tamper attack, anti-replay attack, and resistance against man in middle attack. The method improved flexibility of access control. The encrypted files adopted for storage. Digital signal was used for encryption and decryption process for secure communication. It resisted multiple attacks and guaranteed the system security.

Chang et al. (2016) [11] proposed Cloud Computing Adoption Framework (CCAF) security suitable for business clouds. CCAF multilayered security was based on development and integration of three major securities, such as firewall, identity management and encryption based development of the enterprise files. It Robustness of the CCAF multilayered security was demonstrated. It provided value of volume, velocity and veracity data services operated in the cloud. The Enterprises File Sync and Share (EFSS) security possessed the following issues, such as,

- Employee privacy
- Share link
- Cloud file synchronization
- Enterprise directory integration
The security approach included user storage space modeling, distinct share link, zero knowledge of cloud scale file sharing system, cloud file synchronization, authentication and adoption consideration. The authentication method had advantages of security, flexibility and Single Sign-On (SSO). The system performance was analyzed by precision, recall, true positive rate, and false positive rate. The limitation of CCAF was collaboration and coverage of the testing result. CCAF security policy worked in the real time and it also aligns with the business to protect the data.

Barsoum and Hasan (2013) [8] proposed cloud based enabling data and indirect mutual trust for cloud computing storage systems. It consisted of four features such as it allows outsourced data to dynamic operations, it ensures authorized users, it enables indirect mutual trust between owner and CSP, it allowed owner to grant or revoke the access of outsourced data. The system consisted of four components such as data owner, manage cloud server and provided paid storage space, authorized user, and Trust a Third Party (TTP). It had security requirements, such as confidentiality, integrity, newness, access control and CSP defense. The performance was analyzed by computational overhead, and accuracy. (This work was contained the outsourcing data storages are block level data dynamic, mutual trust, newness, and access control). TTP was able to determine dishonest party. The data owner enforced access control for outsourced data by combining cryptographic techniques were lazy revocation, broadcast encryption, and key rotation. The system analyzed static data with confidentiality requirements. The data storage was supported without excessive overheads in storage, communication, and computation.
Han et al. (2013) [24] proposed the techniques for managing numerous files from the owner to proxy server for shift burden of the identity-based data storage in cloud computing. The cloud computing had the following limitations such as central authority and insecurity against collision attacks. An identity-based proxy re-encryption scheme was the application of the scheme. The collision attack was resisted in inter-domain and intra-domain queries and it provided security. An identity-based proxy re-encryption was implemented to outsource sensitive data from the owner to an external party. They were not employed in the cloud computing. An intra-domain query accessed key was computed with the Private Key Generator (PKG). The owner was independent without the PKG and accessed the one file of the owner instead of all files. The advantage of the model was the security of the system used in the selective identity model. The system was secure against the collision attack.

Khalil et al. (2014) [28] Surveyed on cloud computing security. Clouds had wide range of benefits including configurable computing resources, economic savings, and service flexibility. The security communications had some challenges which depended on multi-tenancy, resource sharing, and outsourcing. These challenges required the ability to cultivate and tune security measures and it was developed for new security policies, models, and protocols. The security problem was solved by vulnerabilities, security trust attacks, neutralized the threats and calibrates the attacks. The twenty-eight cloud security threats were classified into five categories. The no efficient solution was provided against timing side channel attack and energy consumption side channel attack. In public sector, the cloud computing was accelerated to cost reduction factor. The current cloud security issues such as
firewall misconfigurations, malicious insiders, tampered binaries, weak browser security and the mobility was surveyed. The nine attacks identified by the survey are (phishing, fate sharing, botnet, and malware injection). The counter measures of cloud security attack included instruction detection system, autonomous system, and federated identity management system. This system possessed high communication and computational overhead, detection efficiency and coverage.

Zhou et al. (2013) [71] proposed Role Based Access Control (RBAC) scheme for achieving security and encrypted data in the cloud storage. The Role Based Access Control (RBAC) provided flexible controls and management of two mapping. The algorithm was integrated with cryptographic technique. The RBE allowed RBAC policy for encrypted data stored in the public cloud. The hybrid cloud storage architecture allowed the stored data in the public cloud and maintains the sensitive information related to the organization structure in private cloud. The user needed single key for decryption process and system operation was efficient regardless of the complexity of the hierarchy. The RBE included four entities, such as, extract, manage role, add a user, revoke user, encrypt and the decrypt.

Cao et al. (2014) [10] developed multi-keyword ranked search for privacy preserving and encrypted cloud data. The traditional data was based on plain text keyword search before outsourcing. A large amount data and document in the cloud allowed multiple keywords in search request and their reverent keywords. The Multi-keyword Ranked Search over the Encrypted cloud data (MRSE) was used in cloud system. The coordinate matching was the similarity measure of key semantic. The MRSE scheme achieved different privacy requirement in the two different threat
models. The rank search for effective utilization outsourced the cloud data in the aforementioned model. The security was achieved by the multi-keyword ranked then search, privacy preserving and efficiency. The quantitative analysis of query keyword was measured by the inner product similarity. The real data set was provided low overhead on computation and communication.

Sun et al. (2014) [53] developed privacy preserving multi-keyword text search in the cloud supporting based ranking. Encryption was used for protecting user data confidentiality. Accuracy was provided by the search index based term frequency, vector space model with similarity measures. Tree-based index structure was used to improve the search efficiency. The adaptive based multi-dimensional algorithm provided better linear search. Accurate multi-keyword ranked search was used to measure the cosine similarity scores. Keyword privacy breach was possible for the distance pre serving property of BMTS. The search process was adopted by the plain text information retrieval community. Cipher text scenario was implemented in a straightforward manner. The security analysis compiled with the search privacy requirements, such as index confidentiality, query confidentiality, query unlinkability, and keyword privacy. Vector space model with cosine measure effectively procures accurate search result. The privacy requirements included two threat models. The efficiency of the search algorithm significantly improved. The system provided effectiveness, efficiency, and privacy.
2.4 ATTACKS IN CLOUD

Singh and Shrivastava (2012) [50] reviewed various attacks in cloud computing. The biggest issue in cloud computing was security. Here, various types of attacks in cloud computing are surveyed. The attacks in cloud computing were,

- Denial of Service (DoS) attack
- Side Channel Attack (SCA)
- Dynamic Power Analysis
- Simple Power Analysis (Espadas, et al.)
- Algebraic SCA
- Correlation Power Analysis
- Template Analysis
- Stochastic SCA
- Mutual Information Analysis

The cloud computing used three different classes, such as service user, service instances, and cloud provider. Cloud protector of neural network was trained to detect and filter DoS attack. The problem was simultaneously achieved by fine-grained-ness, scalability, and data confidentiality of access was still unsolved. Attack surfaces developed the classification taxonomy by means of four up-to-date attack incidents of cloud computing. The collection and classification of cloud-based attacks and vulnerabilities proved the taxonomy’s applicability and appropriateness. The RSA operation was decomposed by key generation, encryption, and the decryption process.
Data encryption standard (Zhou et al.) used 565-bit key and it for sufficient encrypted sensitive data.

APPENDIX

Figure 2.5 Cloud Computing Triangle and the Six Attack Surfaces

Du et al. (2015) [15] presented the cryptographic analysis of stream cipher MUGI under the cache timing attack model as shown in Figure 2.5. Template attacks used profiling step to compute the parameter of a multivariate normal distribution from the training device an attack parameters obtained the profiling used to infer some secret value on the target device. The attacks achieved the weakness of MUGI cipher that was also used in conduct template attacks. Hamming leakage model has presented the template key recovery attacks of MUGI. A combined cache timing and template attack were used to reduce the computational complexity. Tolerate errors were used in the combined attack. The demerits of the attacks were, to improve the error tolerance of the combined and individual attacks.
Zhao et al. (2013) [68] proposed an efficient hamming weight based Side Channel Cube Attacks (SCCA). The attacks were a combination of both side channel attack and cube attack. The new technologies were used in the non-linear equation and an iterative scheme was used to extract more information from the leakage. Hamming Weight SCCA (HW-SCCA) included the countermeasures such as random delay and masking. The attack was classified into two, such as, preprocessing phase and online phase. Online phases were divided into two, such as, deduced hamming weight and recover the secret key.

2.4.1 Limitation of HW-SCCA

The HW-SCCA provided the software implementation of PRESENT on micro controllers and the HW intermediate states were used for being accurately deduced in the attacks. The extracted cube size was very small and the super poly was simple. The power pattern of different rounds and the operations were easily identified. HW deduction was accurate, the adversaries enumerate all cubes and super polys and then test their relation with cube attacks. The relation holds the key which was recovered bit by bit. Ciphers were classified into three approaches,

- Increased the degree of equation of each output bit
- Make the linear terms in the equations were more complicated
- Increase the number of rounds which was required to the leakage bit with all key bits

The nonlinear equations and iterative scheme were two approaches for improving the SCCA. All the attacks were too easily extended by PRESENT-128.
Seibert et al. (2014) [47] reviewed the side channel attack on the information leaks without memory disclosures and the fundamental assumption behind the code diversity. The attack was used for memory corruption vulnerability to create the side-channel leak information. Side channel attacks on the cryptography were applicable to code diversification. Cryptographic implementation was optimized for certain operation, to reduce the performance cost. It mainly depended on the secret key. The fault analysis analyzed the physical access of control environment devices. The temperature and power supply voltage an attacker induced the fault in the devices. The cache was hit and missed leak information about the data and the code accessed by the process. The cache hit the shorten execution time, the attacker measured the execution time and the memory accessed.

2.4.1.1 Physical Access

Multiple or numerous side channel attack was not performed remotely. The power of Electromagnetic Emanation (EM) and acoustical analyses were required to measure the power consumed, the EM field produced or the sound produced by the devices were respectively. The code diversity was assumed so that attackers cannot read the code. The code diversity raised the bar for the attackers. Side channel attack was against the code bases and the analysis of exploiting the multiple side channel attacks with the same payload.

Prouff and Rivain (2013) [44] proposed the security of masking against the side channel attack. A formal security of the masked was implemented by the block ciphers. The information was gained by observing the leakage of execution was negligible. The side channel attack was a class of cryptanalytic attack. It was called
black box model because it offered more efficiency than cryptanalysis. The attack was classified into side channel attack and continuous side channel attacks. The attacks measured the running time, power consumption or electromagnetic radiation. The continuous channel attack was proved effective especially for breaking the unprotected cryptographic implementation. The continuous side channel attack was against the implementation to provide the security.

Irazoqui et al. (2014) [26] implemented the AES algorithm for data security in transformation. The flush and the reload provided new fine grain attack and recover the whole key. The attackers took advantages of reduplication, so the victim and the attackers shared the same memory. There was more scenario occur the more noise of the attackers. The attack on the native machine was not only preferred, it was preferred the more machine. The attackers have shared the same memory, the VM scenario was used. The lighting fast attack used less time i.e., less than a minute. In AES algorithm was not used in lighting fast attack. The collocation with the encryption server is suited for recovering the key. The AES algorithm was compared with Open SSL 0.9.8. The AES was provided much faster and the trends to be confirmed by the attacks. The algorithm was applied to obtain the cipher text reload vectors. The Flush and reload attackers were only required to monitor a single line memory. Flushing was done before encryption and reloading after encryption.

Thillard et al. (2013) [56] surveyed the side channel attack for their efficiency. It was classified into two, such as divide and conquer. The attack easily tackled the Correlation Power Analysis (CPA). The confidence level of the sub key was no longer. The CPA was evaluated by the notion of the confusion coefficient, capturing
the effect of cryptographic primitives on the difference between correct hypotheses. The confidence level was used to measure their accuracy. The disadvantage of the attack was an acceptable success rate. In side channel attack, the success rate was the central problem. The targeted sub key was used to compare the expressing the success rate as a function of leakage noise. The success of an attack was both contexts between known and unknown correct key. The CPA was compared with the hamming weight leakage model.

Benger et al. (2014) [9] reviewed the side channel attacks in a small amount. The small amount of data from the Open SSL ECDSA used the standard lattice technique. This technique used private key for security. The observed execution was able to make the side channel attack. Relatively a small number of the execution was observed by the private key. A small amount of post-processing is done through lattice reduction. The recovering secret key for the 256-bit curve used 200 signatures. Mathematical calculation used both public and private key. The side channel attack affected the processor architecture and the Intel. The SPY program was used to trace the memory read and execute the access victim program to share the memory pages. It was required to execute the same physical processor as the victim. GLV method was not completely the overall attack but it reduced the effectiveness. It reduced the number of leaked bits but it was not sufficient to prevent the attack. A positive flip side of the attack has used the algorithm for improving the efficiency of the scalar multiplication seems and it reduces the effectiveness of the attack. The scalar blinding technique used the arithmetic operations to hide the value from the potential attackers. The scalar multiplication consisted of fixed window algorithm. The sequence of
memory access does not depend on the private key. The implementation used the sequence memory lines irrespective of the private key.

Liu et al. (2015) [32] proposed the last level cache for effective side channel attack. The techniques achieved high attack resolution without relying on weakness in the OS. The Last Level Cache (LLC) does not require sharing cores or memory between the attackers and victim. The two key techniques were used for enabling efficient LLC based prime and probe attacks. The virtual machine (VM) covert timing channel was high in the measured bandwidth. The key was extracted from secret dependent execution path and demonstrated square and multiply modular exponentiation. The LLC based cross core and VM based prime and probe used the general technique for an attacker to cache set. The probe was the continuous execution and measured the time of each set code that was primed. The attack has monitored the use of squaring operations. The time between subsequent squaring was recovered by the exponent. Trace a cache set was divided into multiple fixed slots. Each probe included with the squaring operation. The victim multiplication operations of the cache set activity created the trace patterns. The capture errors were occurred by noise. The cache set was similar to usage of the multiplier. The size of LLC was smaller than the multiplier, in filter out of unexpected trace pattern. The trace pattern of the cache set used for the same multiplier was identical to the multiplier usage pattern. The attack collected the trace pattern of the multipliers. The clustering algorithm was used in the trace pattern. An actual usage of the multiplier in the multiplication operation occurred in the group trace pattern. The capture errors occurred in the clusters. The correction processes processed the trace pattern from left to right. The low channel capacity, an LLC based side channel leaked the course grain
information. The attacks improved high granularity that was enabled in leaking of cryptographic keys. Preventing the leaks from exponent blinding was divided into modular exponentiation. Constant time was not included in conditional statements. The measure was present in the constant time implementation because the multipliers and the modular reduction was not constant time. Fine-grained resource partition came under the cache partitioning. The attackers cannot extract the useful information because the secure cache designs were randomized the memory to cache mapping. The fixing GnuPG has not prevented the information leaks from other software. Frequently executed secret computation that was not constant time in vulnerable to the attack.

Espadas et al. (2013) [18] developed tenant based resource allocation model for scaling software as a service application. Large applications were deployed over pay per use cloud for high-performance infrastructure, and cost-effective scalability was not obtained because the idle processes and resources were unused. The cloud computing of their multi-tenancy has created cost effective scalable environment. In virtual machines resource utilization were not used. Potential virtual machines and applications were used for measured the resource utilization. Apache meter was open source software of JAVA application and the functional behavior was measured by the performance. The cloud communication layer contained the components for monitoring and accessing the private infrastructure via the SOAP interfaces. The cloud communication layer included two components, such as VM Status handler and VM factory. The model included three complementary approaches namely tenant-based isolation, tenant-based load balancing and tenant based virtual machine instances. The disadvantage of the model was required to statistically.
Zhou et al. (2013) [70] endorsed the schedule vulnerabilities and the coordinated attacks in cloud computing. Multiple Virtual Machines (VM) on single physical system was provided by the hypervisor. The cloud computing services, such as amazon elastic computed cloud (EC2) provided the customer with VM hardware. The credit scheduler provided fairness and low input or output latency for VM and poorly behaved in their fairness guarantees. The user level implementation was used in both user level and kernel-based code. The kernel based implementation user level was problematic, it involved in modified and adding overhead to the application consuming. The malicious customer was limitation was not subjected in the attackers. An extension of the mechanism was a re-usable component such as library or interpreter to incorporate the attack. The general mechanism was implemented in the kernel level version of this attack. The CPU stealing mechanism was able to create the application in any running programming. Kernel Level attack has added the file to the kernel source tree and modifying the kernel configuration to new files. The compact code and the common space for the function were tightly related to the kernel. Loadable Kernel Module (LKM) has allowed the developers to make the changes in the running kernel. Loadable Kernel Modules (LKM) possessed contained some advantages, such as,

- No kernel recompilation
- New kernel functionality was added without root administration
- No reboot was required
- LKM was reloaded at the run time
- It does not add to the size of the kernel permanently
The randomized scheduler was classified into three, such as passion scheduler, Bernoulli scheduler, and the uniform scheduler. The Bernoulli scheduler was used in the Bernoulli processor. It was used for discrete-time analog of the passion process and the Poisson sampling. Schedulers used in the thwarting the attacks. Normal execution was used to modify the scheduler impact. The new scheduler was performed by their testing the latency between two VMs in two configurations, such as,

- VMs were executed on the same core with no other VMs active
- CPU bound VM was added on the other core

The four approaches were utilized to eliminate the cycle stealing vulnerability and demonstrate their effectiveness of attack in the laboratory setting. The disadvantage of the attack was, scheduler offered the minor or no overhead.

Lonea et al. (2013) [34] proposed a technique for the detecting and analyzing the Distributed Denial of Service (DDoS) in the cloud computing. The attackers required the source of cloud services distributions. Instruction Detection System (IDSs) and Virtual Machine (VM) were combined to the cloud system with the data fusion methodology. VM based IDS output alerts were stored into the database placed within the Cloud Fusion Unit (CFU) of the front end server. The flooding attacks mentioned the Fault Tree Analysis (FTA) and the Dempster Shafer Theory (DST). The quantitatively represented the imprecision and efficiently used the IDS for reducing the false alarm rates. The computational complexity of DST was increased exponentially with the number of elements in the frame of discernment. The number of alerts decreases and the conflict generated by the combination of the information
provided by the multiple sensors entirely eliminated. The advantages of the DST were,

- To accommodate the uncertain state
- To reduce the false negative rate
- To increase the detection rate
- To resolve the conflicts generated by the combination of the information

Yan and Yu (2015) [60] evaluated the distributed denial of service attacks in software-defined network in cloud computing. Software-defined networking (SDN) was easy to detect and react the distributed denial of service (DDoS) attacks. Data plane from the control plane of SDN introduced the new attack. The DDoS attacks of cloud computing were based on the characteristics of the on-demand self-service, broad network access, resources pooling, and measured service. The SDN was a good tool to detect the DDoS attacks in the cloud computing. DDoS attacks solved the SDN problems. The SDN created a fascinating problem, such as promising tool to defeat the DDoS attack and versus a vulnerable target of DDoS attacks.

Zhang et al. (2014) [66] proposed the new framework for cross tenant side channel attacks in PaaS clouds. The frameworks have used flush and reload attacks for extracting the secrets in the tenant boundaries. In the commercial clouds, cross tenant and side channel attacks were used. The isolation was classified into four such as,

- PaaS tenant isolation
- User based isolation
• Container based isolation

• VM based isolation

The attack was processed to extract the Advanced Encryption Standard (AES) key used for victim process and it was applied in the running OS. The adversary address space was aligned in the region of the physical memory that was built in the flush and reload attack. The transition function satisfied some constrains line observability, and feasibility. The flush reloads attack was used to reduce the noise. The false positive noise was due to the false sharing of chunks and the hardware cache prefetching process has occurred for sharing the same memory. Co-location in PaaS contained following stages, such as detection, validation and experiments. The side channel attack was demonstrated in the PaaS environments. The key was used in both encryption and decryption process. It provided security for the cloud data. The attackers occurred in the side channel counter measures. The classic Bleichenbacher padding oracle attack used the RSA private key for decryption process.

Ye et al. (2014) [63] proposed non-linear collision attacks based on the side channel attacks. The side channel leakage was hard to characterize with the fixed leakage model. The AES algorithm was used in the linear collision. The classical collision attack was not used in the collision detection to reduce the key hypotheses. Each sub key has not recovered in the linear correlation collision attack (LCCA). The advantage of nonlinear collision has provided the same value of similar leakage behavior. The LCCA was compared with DPA and CPA. The NLCA has not chosen the plain text attacks. The random plain text input provided the known plain text attacks. The nonlinear collision attacks were called collision based side channel
attacks. The leakages of collisions of different states did not provide accurate leakage modeling. It provided low impact performances.

Fei et al. (2014) [19] developed statistics-based model for side channel attack. The SCA was similar to the Correlation Power Analysis (CPA) and the Differential Power Analysis (DPA). In the power analysis, the signal to noise ratio was measured by single bit unit power consumption and the standard deviation of the power distribution. The Maximum Likelihood Estimation (MLE) has used the statistical model for side channel attacks in the physical implementations and the cryptographic algorithm. The model was established by the analytical relations between success rate of the attacks and the cryptographic system. The DPA and the CPA were verified by the AES and the DES, this model was provided the high accuracy and demonstrated effectiveness of the algorithmic confusion analysis.

<table>
<thead>
<tr>
<th>Author</th>
<th>Description</th>
<th>Attack</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Erl et al. 2015) [17]</td>
<td>The cryptographic analysis of stream cipher MUGI under the cache timing attack model</td>
<td>Timing attack</td>
<td>Reduce the computational complexity</td>
<td>Attacks were, to improve the error tolerance of the combined and individual attacks.</td>
</tr>
<tr>
<td>(Yan et al. 2016) [61]</td>
<td>An efficient hamming weight based Side Channel Cube Attacks (SCCA)</td>
<td>Side Channel Cube Attack</td>
<td>HW deduction was accurate</td>
<td>Make the linear terms in the equations more complicated</td>
</tr>
<tr>
<td>(Patel et al. 2013)[42]</td>
<td>Side Channel Attack on information leaks without memory</td>
<td>Side Channel Attack</td>
<td>The cache hits the shorten execution time, the attacker</td>
<td>The code diversity was assumption so the attackers</td>
</tr>
</tbody>
</table>

Table 2.1 Comparison Table
<table>
<thead>
<tr>
<th>Author</th>
<th>Description</th>
<th>Attack</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Sharma and Jha 2015)[49]</td>
<td>disclosures and the fundamental assumption behind the code diversity.</td>
<td>Side Channel Attack</td>
<td>The continuous Side Channel Attack was against the implementation to provide the security.</td>
<td>Success rate was major problem</td>
</tr>
<tr>
<td>(Somani et al. 2015)[52]</td>
<td>The security of masking against the side channel attack.</td>
<td>Side Channel Attack</td>
<td>Fast attack used less time</td>
<td>AES algorithm was not used the lighting fast attack</td>
</tr>
<tr>
<td>(Sharma and Jha 2015)[49]</td>
<td>The attack was easily tackled by the Correlation Power Analysis (CPA). The function of leakage noise and algebraic properties of the cryptographic primitive.</td>
<td>Side Channel Attack</td>
<td>Confidence level was used to measure their accuracy</td>
<td>The success rate was the central problem</td>
</tr>
<tr>
<td>(Liu et al. 2016)[33]</td>
<td>Software defined network in cloud computing. Software Defined Networking (SDN) was easy to detect and react the Distributed Denial of Service (DDoS) attacks.</td>
<td>Distributed Denial of Service attacks</td>
<td>Software Defined Networking (SDN) was easy to detect and react the distributed denial of service</td>
<td>The SDN created a very fascinating problem</td>
</tr>
<tr>
<td>(Haimes et al. 2015)[23]</td>
<td>The attackers required the source of cloud service</td>
<td>Distributed Denial of Service</td>
<td>To resolve the conflicts generated by the</td>
<td>Increase the false detection rate</td>
</tr>
<tr>
<td>Author</td>
<td>Description</td>
<td>Attack</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>distributions. Instruction Detection System (IDSs) and the Virtual Machine (VM) were combined with cloud system with the data fusion methodology.</td>
<td>(DDoS)</td>
<td>combination of the information</td>
<td></td>
</tr>
<tr>
<td>(Perez-Botero et al. 2013)[43]</td>
<td>The multiple Virtual Machines (VM) on single physical system provided the hypervisor. The credit scheduler provided. fairness and low input or output latency for VM and poorly behaved in their fairness guarantees</td>
<td>Coordinated attacks</td>
<td>No kernel recompilation New kernel functionality was added without root administration</td>
<td>Reboot was required</td>
</tr>
<tr>
<td></td>
<td>The techniques achieved high attack resolution without relying on the weakness in OS. The Last level cache (LLC) does not require sharing cores or the memory between the attackers and victim.</td>
<td>Side Channel Attack</td>
<td>An expatiation algorithm to fixed window exponentiation has provided the patch.</td>
<td>It required the trace pattern</td>
</tr>
<tr>
<td>(Younis and Kifayat 2013)[64]</td>
<td>The AES algorithm was used in linear collision. Each sub key has not recovered the</td>
<td>Non-linear collision attacks</td>
<td>The nonlinear collision provided the same value of similar leakage behavior.</td>
<td>Collision attack was not used in the collision detection to reduce the key hypotheses</td>
</tr>
<tr>
<td>(Fernandes et al. 2014)[20]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Author</td>
<td>Description</td>
<td>Attack</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>(Sun et al. 2014)[54]</td>
<td>The SCA was similar to the Correlation Power Analysis (CPA) and the Differential Power Analysis (DPA). In the power analysis, the signal to noise ratio was measured by single bit unit power consumption and the standard deviation of the power distribution.</td>
<td>Side Channel Attack</td>
<td>The high accuracy and effectiveness of the algorithmic confusion analysis.</td>
<td>It was not suited for the detection process.</td>
</tr>
</tbody>
</table>

2.5 SUMMARY

In this chapter, various literature reviews are shown with their techniques and attacks of cloud computing. The Side Channel attack was used the cryptographic algorithm. AES algorithm is used for the same key for encryption and decryption process. This attack provided high accuracy and demonstrated the effectiveness of the analysis. The attack was used to reduce the computational complexity. The Side Channel Attack and their classification such as Simple Power Analysis (SPA), Differential Power Analysis (DPA), Correlation Power Analysis (CPA), Mutual Information Analysis (MIA), and Algebraic Side Channel Collision Attack (ASCCA)
are also discussed. The disadvantages of various attacks are discussed in this chapter and are listed below.

- An attack was required to improve the error tolerance of the combined and individual attacks
- Success rate was major problem
- The SDN was creating a very fascinating problem
- Increase the false detection rate
- Reboot was required
- Attackers was not suited for the detection process