Challenges and Issues in Cloud Security for WBAN applications – A Systematic Survey

B. Gomathy and S.M. Ramesh
1Professor, Department of computer science and Engineering, KPR Institute of Engineering and Technology, India
2Professor, Department of Electronics and Communication Engineering, M. Kumarasamy College of Engineering, India
3KPR Institute of Engineering and Technology, India

Abstract - A systematic and comprehensive review of privacy preserving and security challenges in cloud environment is presented in this literature. Since, cloud supports various applications, it requires immediate attention for serious security and privacy issues. Research must focus on efficient security mechanism for cloud-based networks, also it is essential to explore the techniques to maintain the integrity and confidentiality of the data. This paper highlights research challenges and directions concerning the security as a comprehensive study through intensive analysis of various literatures in the last decade, and it is summarized in terms of architecture types, evaluation strategies and security model. We surveyed, investigated and reviewed the articles in every aspect related to security and privacy preserving concepts and identified the following tasks: 1) architecture of wireless body area networks in cloud, 2) security and privacy in cloud based WBAN, 3) Cloud security and privacy issues in cloud 4) diverse authentication and cryptographic approaches, 4) optimization strategies to improve the security performance.

Keywords - Security and Privacy, Authentication and Cryptography, Optimization, Systematic Review.

1. Introduction

Wireless body area network is a low power intelligent wireless communication technology which could be implanted or attached to human body for continuous monitoring of body [1] under mobility and stationary conditions [2]. Internetworking these devices collects and transmits the information through gateway [3]. The delivered data in monitoring station stores, process and analyse the data using a suitable communication infrastructure [4]. IEEE 802.15.6 standard classifies the wireless body are network applications into two categories such as medical and nonmedical. The medical applications are further categorized into remote control, Implant and wearable applications while the nonmedical applications include real time streaming, entertainment and emergency. Initially, WBAN was implemented for efficient and real time health monitoring [5] systems to help the aging society. Later, the advantages and cost-effective benefits in continuous monitoring and assessment, helps to improve the real time process which makes the WBAN to spread in wide area of applications. Figure 1 depicts the key application of WBAN in detail under various categories [6].
The number of nodes in a wireless body area network ranges from 6 to 256 based on the IEEE standard and a single coordinator may handle 64 nodes. A maximum of 256 nodes may exist for a person if the WBAN has two or more coordinators. The operation topology [7] of WBAN is defined as one hop topology or two hop topologies. In one hop topology the communication is initiated from the device to the coordinator and vice versa. In case of two hop topology, intermediate nodes such as relays are used to communicate between coordinator and nodes.

The recent versions of WBAN are appreciated to design using two hop communication. Apart from topology two modes of communication is exist in WBAN as per IEEE standard such as beacon mode and non-beacon mode [8]. In order to define the boundaries of super frame, the coordinator periodically transmits a beacon to synchronize the nodes in the beacon mode communication. In case of non-beacon mode, Carrier-sense multiple access with collision avoidance is preferred to transmit the data. Based on IEEE standard the following parameters are defined for WBAN communication

- The data rate must be 10kb/s to 10Mb/s and it need to support various WBAN applications.
- WBAN sensors may transmit at up to 1mW which complies with the specific absorption rate of 1.6 W/Kg in 1g of the human body tissue
- Battery life time should be at a span of several months to years based on the methods of implant or attachment.
- 2-5m operating range is prescribed for sensors to communicate with each other in the same body.
- Latency should be <125ms for medical applications and 250ms for nonmedical applications.
- Energy efficient data transfer with minimum delay must be preferred in WBAN which should guarantee the data transmission.
- WBAN should be configurable so that individual nodes could join the system without any external process.
- WBAN should coexistence with other wireless technologies like Bluetooth, WSN, ZigBee and WLAN etc.

**WBAN Architecture**

WBAN is a three-tier communication model [9] in which Tier-1 is an intra WBAN communication which provides communication between the sensors and the hub. It is approximately 2m around the body to collect the data and forward to a personal server or gateway [10]. Tier-1 is considered as Intra WBAN communication. In Tier-2 Inter WBAN communication is performed between the hub and access points. Several networks are interconnected to WBAN in the Tier-2. The major function is to transmit the data to gateway through secured communication protocol. The connection between Tier-2 and the remote server is established in Tier-3 through internet. [11] Remote server is designed based on the application to collect the information. Figure 2 depicts the communication tiers in WBAN. In the communication model, Tier-1 is considered as challenging component since its radio wave communication is affected by human body effects. Compared to other wireless sensor networks the intra WBAN communication is most challenging one. The design considerations applied to WBAN is characterized based on parameters such as data rates, transmission power, communication range, latency, mobility, configuration and coexistence.

Cloud computing refers to the applications or services processed over distributed network by utilizing the virtual resources [12]. These common resources are accessed through basic internet protocols and networking standards. It provides virtual and boundless resources which could be accessed by end user through prescribed applications. Integrating cloud with WBAN requires on-demand, scalable, secure storage processing infrastructure [13]. This hybrid platform process large amount of data which is collected through sensor nodes. The collected data must be transmitted with minimum delay and power [14]. Figure 3 depicts the integrated architecture of cloud enabled WBAN in medical application [15].
Cloud providers have robust infrastructure which includes servers, routers and more components to provide essential service to the user. It requires high scale devices for different applications to meet the economic and technical requirements. The recent development in low-cost devices helps to integrate the WBAN with cloud is complex to realize. Two important parameters are considered in case of WBAN such as nodes and transmission rate in terms security and privacy [16],[17]. Node security is essential so that the generated or collected information could be preserved from intruder. Transmission rate plays another vital role since if the data encryption or decryption is performed in the data before transmission to preserve its uniqueness if affects the transmission rate. Generally, sensors are used as nodes and the transmission rate may increase or decrease due to environmental changes which affects the performance of the system. This leads into data degradation or loss so that an intelligent resource allocation and management system is required to implement cloud based WBAN. Integrating cloud with WBAN has various advantages such as

- Integrating cloud with WBAN provides wide functionalities and services based on the requirements of application such as video streaming, data mining, etc.,
- Reduces the limitation in bandwidth requirements since the integrated architecture deploy the services and enhance the efficiency in terms of communication, computation, storage and power.
- Strong privacy and security protection could be enabled in the integrated architecture due to its flexible services,
- Cloud has multiple backups of data, so that the reliability is much better than conventional wireless sensor networks. The application will run continuously in cloud without any interruption.

There are few limitations present in integrating cloud with WBAN as follows

- Cloud doesn’t have self-governing nature to adapt with WBAN nodes and its transmission rates.
- Increased number of clouds in a region simultaneously increases the delay and transmission power.

2. Literature Survey

In this section vast survey has been made by analyzing various research models in terms of cloud security and privacy, integrated architecture models, authentication, cryptographic approaches and optimization straggles used in cloud. Special attention required while handling data in cloud and the trust of entire system depends on the data prevention techniques. Numerous tools have been introduced and tested by researchers for efficient data protection and prevention of unauthorized access. Still the gap needs an attention to sort it through a better data prevention and protection technique.

3. Cloud Service Security

Security issues in cloud service model is categorized into

- Network level security issues
- Data level security issues
- User authentication level security issues
- Generic security issues.

Service level cloud security models [18] has its own limitations and before understanding the issues the relationship between the service models is essential. Cloud has three service models such as SaaS [19], PaaS and IaaS [20]. In that the security breach over the IaaS will affect the other two models since they are hosted over the IaaS. Generally, PaaS offers a platform to build an application and SaaS offers deployment platform to the application which increases the security. Because of these dependencies of three layers in cloud, if any attacks or breaches occurs in the network the entire environment will be at risk.

Security Issues with SaaS

In the three cloud service models SaaS has less control over security. It provides services to business applications, communication software and emails. Based on the applications the security factors are analysed in SaaS as follows.

Data security is the major challenge in SaaS platform as the service providers need to concern over the user data security. Based on the control measures and technologies it classified into three sections as

- Protection of data in cloud on migration [21]
- Protection of data between cloud and different service providers [22]
- Protection of data within the cloud [23]

SaaS has the responsibility to secure the data from collection till storage and analyse the data. Most of the organizational data are processes as plaintext in cloud and faces critical issues while handling backup and recovery process. Also, service providers need to concern over the disaster management to ensure the data security. But most of the agreements are complex for service providers due to data location and service provider’s data centers which introduces issues in data security and privacy.

Most of the cloud services are facilitated as applications to users and it is typically processed over internet and web browsers. The possibilities of vulnerabilities in web-based applications are more compared to other processing technologies. Conventional security mechanisms could not
ensure the security and privacy of the data [24]. So, it is essential that new approaches need to be evolved to prevent the security threats and malicious activity over the data in web services.

Another security issue in SaaS is multi-tenancy. Cloud provides service as shared platform and this multi-tenancy [25] has flaws that other users in the network could see the operation of user and trace the residual data. Since multiple tenants and their data are stored in the same database this leads into leakage of privacy information and the risk of data theft which leads into serious issue. So, it is essential to ensure the data security when the resource is shared to other users in the network. Service providers need to handle the issue by implementing security policies to protect the user data from other customers.

Accessing the resource through specific application over internet may expose serious security issues in cloud [26]. Since the user has able to access the network devices which includes personal and public computers and mobile phones etc., which creates a way to intruder to obtain the data. Cloud security alliance provides a list of threats such as stealing information through malware, insecure network connection, OS based vulnerabilities, official applications and other proxy-based security threats.

### Security Issues with PaaS

PaaS is an integrated environment which offers the user to develop, test and deploy the application to support customers. Two layers of security are comprised in PaaS such as

- PaaS platform security [27]
- Application deployed in PaaS platform [28]

The platform service provides must ensure the safety of software which has runtime engine which runs over the user applications. Since the user are dependent over web hosted development tools and other services the PaaS must provide suitable security measure. Combing one or more source elements as an integrated system PaaS must ensure the safety of the data as well as network. Since the components which are changed in PaaS platform to secure the user data and network the complexity of building application over PaaS must be considered by the developers. Also, the developers need to manage the issues related to data storage location. Even though the developers and service providers considering these facts the security issues in PaaS are still exist and researchers work on it to obtain secured model.

The security over access control mechanism in PaaS is present in its delivery model [29]. The CSP in PaaS is responsible for network management, server management and infrastructure management of application over the platform. The customer is also responsible to access the resource [30] through the application developed in platform which has access management to ensure the security through authentication of the users.

### Security Issues with IaaS

IaaS provides resources such as storage servers, networks and other resources as a virtualized system through internet. IaaS has better security concern over other models by controlling the software running in virtual machine. Using suitable security and configuration policies the privacy and security of the system is ensured in IaaS model by cloud service providers. Compared to PaaS and SaaS the security standard is much better in IaaS [31] by providing full access to the user through VM host which is isolated from other systems using hypervisor technology. Hypervisor [32] in VM is used to isolate the VM from other systems. Generally, it is referred as virtual machine monitor which is low level software that controls the VMs. If the security of hypervisor is breached that leads into data expose to all domain so that attacker could migrate the VMM model into malicious server would leads into serious issue. Generally, it is advised to place the VMM as much as small in size which reduces the risk of vulnerabilities and easy to fix if anything happens. Since the malicious VM could capture the information from other VMs as the cloud uses shared memory concept. Similarly, the utilization of convert channels in VMs by passes all the rules in security model of VMM could help the intruder to monitor the resource without known to the VMM. So that the user is responsible for maintaining the system from security threats [33]. IaaS undertake efforts to reduce the security threats from communication, modification, monitoring and mobility of the user data, application. Few important threats under public IaaS [34] are attacking unpatched or vulnerable service over standard ports, hack the account with minimum secured or weakly secured account, key theft to access the control over host, deploying Trojans through software embedded in VM [35],[36] break the system which has not properly configured or secured by firewalls.

Virtualization [37] is a platform which allows the user to roll the virtual machines to run over variety of applications. It creates opportunities to intruders to break the security. Breaking the security in one VM affects the entire VMs in the network as the environment is similar to normal infrastructure. This gives more challenge in security [38] and interconnection complexity. Trojan is one of the security issues and in this an attacker with valid credentials create an image which includes malicious code and sent to the user in the network. If the image is used by another user, then the VM and its data are affected by hidden malware which leads into data breach. In some cases, data leakage could be happened due to VM replication [39]. Since in replication all the information such as passwords, cryptographic keys are recorded as image and if the image is not cleaned after replication [40], that data could be used by another user.

Virtual Networks [41],[42] are responsible for VMs interconnectivity and it secures the VM by connecting the user with physical channel. But most of the hypervisor uses virtual networks to connect VM directly using configured networks such as bridge or routed models. These models are efficient but it creates possible ways to attackers to capture the information. Some of the famous attacks in virtual networks are sniffing and spoofing.
Table 1: Features of cloud deployment models

| Deployment Model | Service management | Infrastructure Management | Infrastructure Location | Access and control |
|------------------|--------------------|--------------------------|------------------------|--------------------|
| Public           | Third party service provider | Third party service provider | Off–premise | Untrusted |
| Private          | Organization       | Organization             | On-premise Off–premise | Trusted |
|                  | Third party service provider | Third party service provider | On-premise Off–premise | Trusted |
| Managed          | Third party service provider | Third party service provider | On-premise | Trusted or untrusted |
| Hybrid           | Both Third party service provider and organization | Both Third party service provider and organization | On-premise Off–premise | Trusted or untrusted |

4. Attacks in Cloud

Though cloud has various advantages it also brings risks to technology adopted organizations. Most of the security threat are performed for data and resources over the delivery model and deployment model as shown in Table 1. Compared to public cloud, private cloud achieves much high security level. As the utilization of cloud data increases every day various types of attacks are increases to know the information of other user. Generally, threat is referred as a potential attack which is performed to access the user information or resources, in contrast vulnerability is referred as flaws in a system which allows the attacker to perform action over the system successfully. Some of the important attacks in cloud data is briefed as follows.

Cross site scripting XSS attacks [43] is performed in client side through some malicious scripts which is introduced by the attacker through website or application. XSS is the most familiar web application vulnerability utilizes the un-valid or un-encoded user input to generate an output. This results into projection of unrelated webpages to the user input. Also, the intruder uses a string along with website as victim browser to access control over the user. Around 84% of security vulnerabilities [44] are carried out by cross site scripting as per the Symantec survey. Cross site scripting is classified into two types such as persistent and non-persistent [45]. In persistent type, the attacker saves the data permanently in the server and displayed it as a normal page to other users. In case of non-persistent, they are provided to the user as commonly as HTTP query parameter which is used in server-side scripts to display the results without sanitizing the user request.

Malware injection attack [46] in cloud computing performed by attacker in virtual machine or implemented application. These types of attacks result into data modification, blocking and changes in its functionalities. Intruder creates an implementation model [47] and included in the cloud network and cracks the VM. Once the action is completed successfully, the system automatically redirects the user requests to malicious system and the codes are executed. This leads into serious security issue in cloud.

SQL injection attack [48] is common in cloud. In this attacker insert some malicious code into standard code to gain access over the database and sensitive information. Since the attacker query is similar to user query and the website allows the user to access the SQL server. This helps the intruder to know the functionalities of website and they could change it as per their requirement [49]. To check the SQL injection attacks in cloud various filtering methods are available to filter the user input, prevention methods to avoid the execution of intruder generated SQL codes. In some research models proxy-based architecture is used to prevent SQL control sequence [50]. Web based intrusion detection systems are used to differentiate authentic events arising in the cloud from the prohibited ones [51]. With low false alarm rate and high detection rate, intrusion detection systems detect harmful codes in cloud computing.

Another popular attack in cloud is Man in the middle attack [52], where the intruder tries to intrude in between the communication and injects false information and obtains the important information from the communication. Cloud requires strong encryption technology to prevent this attack and dSniff [53], CAIN [54], ETTERCAP, AIRJACK etc., are some of the technologies available.

Denial of service [55],[56] is an attack which makes the user not to avail the resource on demand. The request is
temporarily or indefinitely interrupted by the intruder and suspend the service to the user. There are two types of attacks in denial of service such as crash services and flood services. Distributed denial of service [57] is performed the same over thousands of IP addresses. In order to induce denial of service attack multiple systems are targeted in cloud and corrupted in distributed denial of service. The target of DDoS is to attack servers like banks, payment gateways, etc., which can take inefficiencies in web application and it is difficult to identify over the network layer. Various protection measures like cloud based and proxy-based solutions are introduced to reduce the attack intensity [58] by including HTTPD, MySQL server etc., Permanent denial of service is another type of attack that damages the system which requires reinstallation or replacement of hardware [59]. Permanent denial of service accesses the remote administration over the interface of user hardware and other networking elements and modify the firmware with corrupted image and makes the device unusable until it is replaced or repaired.

Buffer overflow attack [60] occurs in cloud if the data is stored beyond its capacity. Generally, a portion of adjacent memory is used to store various types of data and lack of validation of data results into excess data overflow or data overwriting. This makes the system into more vulnerable to attacks and it allows the intruders to deploy the necessary programs [61] which leads into damage. Successful overflow vulnerability leads into changes into memory variable and gains full control of host.

Insecure application programming interface [62] in cloud target to breach a network. Programming interface are provided to users by service providers to manage the data in cloud. Attackers act as common door in application and access the system externally and take over the information. This happens in cloud due to poor authentication and encryption systems. Initially the logs from the application are collected then it can be used to integrate with database to find the necessary resources.

As shown in Table 2, Malicious insider [63] refers to a person or business partner authorized to access data using his privileges. It is not known to the network firewalls and other detection system due to authorized access. Compared to other data breaches, malicious insider causes more security damage and it could affect large number of users. There are two types of threats in insider attack [64] such as inside the cloud service provider and threats from outsourced cloud. If the intruder is working for the service provider and causes damage to security of user data, the impacts could not be measured. It creates much counter issues over service provider and client side. If a part of cloud is outsourced [65] and data breach will occur in the cloud due to insider this threat is outsourced threat. Based on client or service provider side using suitable intrusion detection system the risks in malicious insider attack could be reduced in cloud.

Table 2: Security threats in cloud computing

| Threat        | Types                                                                 |
|---------------|------------------------------------------------------------------------|
| **Confidentiality** |                                                                     |
| Inside user attack | Malicious cloud user belongs to same service provider or another user or third-party user in the network. |
| External attacker threat | software attack of cloud infrastructure software attack of cloud applications hardware attack against the cloud software and hardware attack against cloud user organizations’ endpoint software |
| Data leakage | security access rights failure across multiple domains electronic and physical transport systems failure in cloud data and backups |
| **Integrity** |                                                                     |
| Data segregation | Mismatched security parameters Improper configuration of virtual machines and hypervisors |
| User access | Identity and access management procedures |
| Data quality | Faulty application or infrastructure components |
| **Availability** |                                                                     |
| Change management | Infrastructure changes upon cloud provider, Network bandwidth distributed denial of service Network DNS denial of service Application and data denial of service |
Advances in Computing, Communication, Automation and Biomedical Technology

| Physical disruption | Disruption of cloud provider IT services through physical access |
|---------------------|-------------------------------------------------------------------|
|                     | Disruption of cloud customer IT services through physical access  |
|                     | Disruption of third-party WAN providers services                   |

Exploiting weak recovery procedures

Invocation of inadequate disaster recovery or business continuity processes

5. **Cloud Authentication Attacks**

Authentication is the process which confirms the identity of the user credentials. If the user needs to access information authentication is the first step to prove the right access to resource. In cloud similar procedure is followed, the user has to establish the connection through his credentials to access the cloud resource [66]. Based on the facts in cloud, some of the important authentication attacks are listed as follows.

- **Brute Force Attack** [67],[68]– In this attack the intruder tries to find the credential of user by guessing.
- **Cookie Replay Attack** [69] – Cookies are accessed by an attacker which is stored by user for reuse leads into series security threat.
- **Credential Theft** [70] – By data theft, intruder gains access to the system credentials
- **Dictionary Attacks** [71] – Based on the dictionary terms intruder tries to guess the credentials
- **Network Eavesdropping** [72] – by reading the network traffic intruder gains the credentials.

*Encryption and Authentication in cloud security*

Even though cloud adopting cloud has various advantages still it has some barriers in its security issues. Some of the significant issues and technologies which are related to cloud privacy and compliance issues are discussed in this section. Some of the existing technologies are listed as follows.

Trust based security [73] assessment model for IaaS is considered as reference model for various security and cloud assessment models. Cloud trust estimates the security metrics in terms of confidentiality and integrity of the cloud service provider and computing systems. To assess the security level of multitenant architectures [74] and probability of high value data, a minimal security control is used in cloud trust. This security architecture protects the virtual machines and strengthens the cloud service providers. Also, it reduces the cloud network monitoring and live VMs discovery. The issues identified in IaaS platform using optimized fair pricing scheme are, the profit is often denied mutually between the service providers and users [75]. Also, the maintenance cost is high. Later biometric encryption is introduced to improve the cloud security. But the issue in biometric encryption is in its data as it requires a separate processing and storage units to process the functionalities. Signature based models are evaluated to reduce the central authority and trusted setup environment. Using large class of predicates and standard assumptions the access the provided to the user. The limitation of the signature-based model is present in its computational overhead. Though cloud service providers tried to reduce the computations through outsourcing [76] which leads into untrusted sign in problems.

Multi-factor authentication [77] is used to validate the user in two or more approaches. Generally, two stage authentications are preferred. The first stage consists of user password and the second stage has hybrid profile-based authentication which is recommended based on user behaviour. Later authentication models are evolved with intrusion detection system [78] which provides superior security with minimum computation cost to cloud user and service providers. Using single private key, the user can access the resources from multiple servers. The advantage of the ID based authentication model present in its bilinear cryptosystem pairing [79] and key generation. User authentication and key agreement [80] enables the user to authenticate anonymously and provides connection through secure channel between the user and service provider. The user and server may know the information exchanged and the real identities are nor revealed to the senders which improve the security [81]. Mutual authentication system [82] based cloud authenticates the user and server each other using steganography [83] as an encryption method. Using secret key sharing the authentication is performed and it allows the user and the server to keep a part of key with each other. When it is combined it provides a complete security and it provides flexibility to user to change the key whenever it is required.

Various attribute-based encryption methods [84],[85] are involved to improve the cloud security. Using set of descriptive attributes, the user decrypts the information only if the identity is same as specified by the sender. It there is identity overlaps based on set of threshold values the operation is performed. It could be either denial of resource or grant the resource, it depends on the threshold values and it is suitable for typical applications only. Based on the set of user attributes the encryption [86] is further classified into key policy attribute-based encryption and control policy attribute-based encryption. In KP-ABE [87], based on access policy the sender has to encrypt the data associated with cipher text. Once the sender defined the attributes to define the keys it could not be revoked. Using the same attributed and keys the receiver has to authorize the data and decrypt it using matching attributes. The limitation of KP-ABE is its access policy and secret key as the data owner cannot choose the cipher text to decrypt the data and data owner must rely over the sender attributes. Non-monotonic...
advances in cloud security

Machine learning algorithms in cloud security

6. Machine Learning Algorithms in Cloud Security

Machine learning algorithms [91] are the basic model which performs operations based on their learning behaviour. Machine learning models in cloud computing is used for data mining and classification process. Some of the researchers implemented ML in threat detection and prevention measures [92]. Machine learning computes the results automatically based on experience. Some of the important machine models are Support Vector Machine (SVM) [93],[94], Expectation Maximization, Decision Tree, Naive Bayes Tree classifier [96], Adaptive Neuro Fuzzy Inference System [97],[98], fuzzy C-means Clustering [99] [100], Linear Regression (LR) [101] and Random Forest (RF) [102], Artificial Neural Network [103],[104] and genetic algorithms [105]. Some of the existing models are reviewed in this section based on cloud security.

Support Vector Machine (SVM) is widely used in cloud security since it is insensitive to data dimension and able to produce results with high training rate and decision rate. Due to better learning ability SVM is used as intrusion detection system to improve cloud security [106]. The limitation of SVM model in cloud security present in its limited binary classification process. Though it identifies the attack, SVM model lags in identifying the attack type and consumes more training time. Decision tree-based security models are evolved to handle large data sets. It provides high detection rate compared to SVM due to its inherent characteristics. Tree induction algorithm [107] are used to learn the intrusion patterns and used to classify the network activities over the network data. With feature reduction and combination of decision tree with genetic algorithm [108] provides better performance in reducing the false alarm rate. Decision trees are computationally intensive to build which is considered as the limitation of the model.

Bayesian network or classifier is suitable for intrusion detection applications which needs prior knowledge about the data and attack type. Based on the variables of interest Bayesian networks encodes the probabilistic relationships is the added advantage. Bayesian networks lags in performance while handling continuous features and if the prior knowledge about the data and system is incorrect. Fuzzy based intrusion detection system is proposed in literature [99]. Fuzzy c means clustering is widely used in most of the intrusion detection system in cloud computing [98]. Higher order fuzzy c means algorithm is used to cluster the heterogeneous data and each data object is represented as tensor with its correlation values. Implementing fuzzy model with encryption scheme such as homomorphic encryption [109] improves the security performance. Also, fuzzy clustering is used as [110] conventional privacy protection methods to secure the sensitive information. Using kNN [111] and map reduce model with fuzzy clustering reduces the data dimensionality and reduces the risk. [112] Distributed fuzzy c means clustering algorithm is proposed in the research model to achieve better decision and the security is enhanced over the encrypted data through homomorphic encryption. Implementing virtual nodes over private server helps to detect the intruder attack. The limitation of fuzzy model is its high resource computation. It lags in updating the subsets at runtime which affects the security performance.

Neural network is used in cloud security to find novel and unknown intrusions. Neural network models do not need any expert knowledge in identifying the threats and attacks over the network. Moreover, it is capable of processing noisy, incomplete and limited data which is widely used in various cloud security models. Artificial neural network is widely used in cloud security to detect various types of threats and security breaches. In particular back propagation based supervised learning model [113] is used in various research models. It assesses the network error based on the modified weights. Due to its hidden layer, nonlinear models could be developed which helps to identify the complex relationship between the attributes and classification labels. Later recurrent neural network and deep convolutional neural networks [114] are evolved to classify the tasks along with intrusion detection. Though ANN based IDS models are better, it has some limitations such in its detection precision and accuracy. Since the dataset used in training model is small and it is difficult to identify all the properties of attack. Due to this detection accuracy gets reduced and low frequency attacks could not be identified by ANN models. The limitation of neural network is its over fit nature during training and slow training process. Other than this models, expectation maximization, linear regression and random forest models are used to improve cloud security. Other than supervised learning models in cloud security, few research models are evolved based on semi-supervised learning techniques. It eliminates the attacks in side channels and reduces co-resistance attack by analysing the cluster and improves the security in cloud.
7. Optimization Models in Cloud Security

Optimization models to improve cloud security is proven in various research works by implementing suitable intrusion detection system [115]. Initially trusted based environment is used to measure the performance of virtual machine and identifies the threats. Later hybrid optimized cost scheduling models are introduced to obtain the resource identity, so that the resource could be added to private cloud for execution with in the stipulated time [116]. Optimizing the cost of resource allocation in cloud computing is developed to allocate the resource automatically and identifies the attacks in various cloud infrastructure layers [117]. Fast flux swarm network optimization [118] is introduced in cloud to detect the denial-of-service attack. Improving the cloud security is achieved by efficient resource allocation is implemented through resource optimization in IaaS system which works based on two online resource allocation models. Double molecular structure based chemical reaction optimization [119] is introduced to formulate the scheduling process in acyclic graph jobs provided optimal solution to the cloud issues. For data intensive computing environment various algorithms like particle swarm optimization, genetic algorithm, multi-start PSO and multi start genetic algorithm are introduced.

To improve the performance of cloud-based healthcare systems, meta-heuristic algorithms are developed which preserves the patient and helps to improve the communication. Later private proxy re-encryption is introduced along with heuristic models [120] to reduce the computational complexities in cloud which improves the cloud security. Based on hybrid architecture of cloud scheduling [121] applied meta-heuristic-based security aware model is developed to improve the efficiency of the cloud. In few research models optimizing the sampling size of cloud data is performed to manage the network which reduces the possibility of vulnerabilities in cloud computing. Self-configuring adaptive framework is introduced to optimize the resource allocation in cloud. Similarly, co-evolutionary negotiation algorithm [122] is also implemented in few research models to improve the QoS based on security and resource allocation measures. User side optimization is proposed in research model to improve the service provision to user from service provider. Based on physical layer security in heterogeneous cloud this optimization model improves the cloud user security over attacks. Hadoop [123], Map-reduce [124] and spark [125] based optimization is introduced in cloud to monitor and detect the threats.

Genetic algorithm plays vital role in cloud security and data mining applications of cloud [126]. Various research models are evolved to improve the cloud security using genetic algorithm. Later modification in conventional genetic algorithm is introduced to enhance the performance. Game theoretic based GA [127],[128] is introduced to validate the performance of cloud. Nested genetic algorithm [129] is used in few research models to track and maximize the network reliability and server assignment issues in cloud. To improve the performance of classification model’s genetic algorithm and PSO based combination are used in few research models which provides better computing elasticity to cloud and improves the security by detecting the service attacks. Evolutionary PSO based models are familiar to cloud for its adaptive mitigation reaction and intrusion detection performance over threats and vulnerabilities. Later improved PSO models are introduced to improve the detection performance through its linear programming nature.

Machine learning models are better in intrusion detection and optimizing the machine process through various models like particle swarm optimization, ant colony optimization [131],[132] artificial bee colony optimization [133],[134] bat optimization algorithms [135],[136] cuckoo search optimization algorithm [137] are implemented in cloud network to improve the security performance. These optimization models improve the performance of cloud in terms of efficient task scheduling, resource allocation and intrusion detection and prevention. Ant colony-based models are evolved to improve the scheduling performance and security parameters over multiple data handling platforms. For efficient cloud service computation artificial bee colony optimization is used in few research models. Cuckoo search optimization-based models are used in cloud to improve the security coverage over the network. Other than nature inspired models few mathematical models are evolved as multi objective optimization models [139],[140] [141],[142],[143] which performs better in disaster recovery in cloud environment.

8. Findings from The Survey

Based on the intensive study of existing research works the following points are identified for cloud security is summarized as follows

- Rapid development of cloud technology leads into serious network and data security issues.
- Protecting user data in cloud is a challenging issue as the resources are shared as multi-tenant process.
- It is necessary to design and implement suitable detection system to detect the threats in the network.
- Detection of indirect access to user data such as malicious insider attack is a challenging task in cloud.
- Most of the access control mechanisms are centralized in nature except attribute-based encryption.
- Using encryption in authentication increases the operating cost while performing decryption, key pairing and decryption of cipher text.
- The access policies in existing schemes are not supportable to multiple reads, write operations.
- Utilization of single key distribution in cloud is difficult to support large number of users.
- Development of machine learning techniques for fast threat detection is a challenging task.
- The limitation of machine learning algorithms must be reduced in detection and categorization of attacks in cloud.
Advances in Computing, Communication, Automation and Biomedical Technology

- Optimization models are better in scheduling and resource allocation performances.
- Hybrid optimization models perform better in cloud QoS improvement factors.
- Least number of optimization models are evolved in terms of cloud security and intrusion detection system.
- Traditional methods could not able to identify and provides solution to security threats completely. So, it is important to develop an efficient system to identify and exterminate the security threats.

9. Conclusion
This survey paper is prepared to address the various security issues in cloud and the possible solutions through existing techniques such as cryptography, machine learning based intrusion detection and prevention, optimization models in cloud security. The challenging issues are analysed and presented in detail. Based on the survey we infer that optimization-based models are the recent trend in cloud security which handles various challenges. Based on this factor we conclude that optimization models will play a significant role in threat detection and attack prevention in future cloud computing environment.

References
[1]. Keisuke Hachisuka, Azusa Nakata, Teruhito Takeda, Kenji Shiba, Kiyoshi Iiao, “Development of wearable intra-body communication devices” Sensors and Actuators A: Physical, Vol.105, No.115, pp.109-115.2003.
[2]. Poon.C.C.Y., Yuan-Ting Zhang, Shu-Di Bao, “A novel biometrics method to secure wireless body area sensor networks for teledermecine and m-health” IEEE Communications Magazine, Vol.44, No.4, pp.73-81.2006.
[3]. Okundu Omeni, Alan Chi Wai Wong, Alison J. Burdett, Christofer Tournazou, “Energy Efficient Medium Access Protocol for Wireless Medical Body Area Sensor Networks” IEEE Transactions on Biomedical Circuits and Systems, Vol. 2, No. 4, pp. 251-259.2008.
[4]. Elisabeth Reusens, Wout Joseph, Benoît Latré, Bart Braem, GÜnter Vermeeren, Emmeric Tanghe, Luc Martens, Ingrid Moerman, Christ Blondia, “Characterization of On-Body Communication Channel and Energy Efficient Topology Design for Wireless Body Area Networks,” in IEEE Transactions on Information Technology in Biomedicine, Vol. 13, No. 6, pp. 933-945.2009.
[5]. Mark A. Hanson, Harry C. Powell Jr, Adam T. Barth, Kyle Ringenberg, Benton H. Calhoun, James H. Aylor, John Lach, “Body Area Sensor Networks: Challenges and Opportunities” Computer, Vol.42, No.1, pp.58-65.2009.
[6]. Maulin Patel, Jianfeng Wang, “Applications, challenges, and prospective in emerging body area networking technologies” IEEE Wireless Communications, Vol.17, No.1, pp.80-88.2010.
[7]. Daniel Bauer, John N.Daigle, IliasIliadis, PaoloScotton, “Topology aggregation for combined additive and restrictive metrics”, Computer Networks, Vol.50, No.17, pp.3284-3299.2006.
[8]. Jacejoon Cho, Sunshin an, “Optimal beach scheduling mechanisms using cluster identifier for healthcare application” Expert Systems with Applications, Vol.36, No.3, pp.5071-5080.2009.
[9]. Aleksandar Milenković, Chris Otto, Emil Jovanov, “Wireless sensor networks for personal health monitoring: Issues and an implementation” Computer Communications, Vol.29, No.13–14, pp.2521-2533.2006.
[10]. Emil Jovanov, Carmen C. Y. Poon, Guang-Zhong Yang, Y. T. Zhang, “Guest Editorial Body Sensor Networks: From Theory to Emerging Applications” IEEE Transactions on Information Technology in Biomedicine, Vol. 13, No. 6, pp. 859-863.2009.
[11]. Chunqiang Hu, Hongjuan Li, Yan Huo, Tao Xiang, Xiaofeng Liao, “Secure and Efficient Data Communication Protocol for Wireless Body Area Networks,” IEEE Transactions on Multi-Scale Computing Systems, Vol. 2, No. 2, pp. 94-107.2016.
[12]. A. Haldorai and A. Ramu, “Security and channel noise management in cognitive radio networks,” Computers & Electrical Engineering, vol. 87, p. 106784, Oct. 2020. doi:10.1016/j.compeleceng.2020.106784
[13]. A. Haldorai and A. Ramu, “Canonical Correlation Analysis Based Hyper Basis Feedforward Neural Network Classification for Urban Sustainability,” Neural Processing Letters, Aug. 2020. doi:10.1007/s11063-020-10327-3
[14]. Sana Ullah, Athanasios Avlakos, Han-Chieh Chao, Junichi Suzuki, “Cloud-assisted Wireless Body Area Networks” Information Sciences, Vol.284, pp.81-83.2014.
[15]. Miguel S. Familiar, José F. Martínez, Iván Corredor, Carlos García-Rubio, “Building service-oriented Smart Infrastructures over Wireless Ad Hoc Sensor Networks: A middleware perspective” Computer Networks, Vol.56, No.41, pp.1303-1328.2012.
[16]. Hua-Pei Chiang, Chin-Feng Lai, Yueh-Min Huang, “A green cloud-assisted health monitoring service on wireless body area networks” Information Sciences, Vol.284, pp.118-129.2014.
[17]. Jiafu Wan, Canfeng Zou, Sana Ullah, Chin-Feng Lai, Ming Zhou, Xiaofei Wang, “Cloud-enabled wireless body area networks for pervasive healthcare,” IEEE Network, Vol. 27, No. 5, pp.56-61.2013.
[18]. Nguyen Dinh Han, Lõnghe Han, Dao Minh Tuan, Hoh Peter In, Minho Jo, “A scheme for data confidentiality in Cloud-assisted Wireless Body Area Networks” Information Sciences, Vol.284, pp.157-166.2014.
[19]. Ling Mi, Wenjing Lou, Kui Ren, “Data security and privacy in wireless body area networks” IEEE Wireless Communications, Vol. 17, No. 1, pp.51-58.2010.
[20]. Steve Mansfield-Devine, “Danger in the clouds” Network Security, Vol.2008, No. 12, pp. 9-11.2008.
[21]. Gene K Landy, “Software as a Service (SaaS)” The IT Digital Legal Companion, pp. 351-374.2008.
[22]. Jianhua Che, Yamin Duan, Tao Zhang, Jie Fan, “Study on the Security Models and Strategies of Cloud Computing” Procedia Engineering, Vol.23, pp.586-593.2011.
[23]. Wu Shengqi, Zhang Shenglong. Kong Lanju, “Schema Evolution via Multi-Version Metadata in SaaS” Procedia Engineering, Volume 29, pp.1107-1112.2012.
[24]. Changlong Tang, Jiagiang Liu, “Selecting a trusted cloud service provider for your SaaS program” Computers and Security, Vol.50, pp.60-73.2015.
[25]. Vidyhalakshmi, Vikas Kumar, “CORE framework for evaluating the reliability of SaaS products” Future Generation Computer Systems, Vol.72, pp.23-36.2017.
[26]. Ricardo Martins, Tiago Oliveira, Manoj A. Thomas, “An empirical analysis to assess the determinants of SaaS diffusion in firms” Computers in Human Behavior, Vol.62, pp.19-33.2016.
[27]. Stefan Walraven, Dimitri Van Landuyt, Eddy Truyen, Koen Handekyn, Wouter Joosen, “Efficient customization of multi-tenant Software-as-a-Service applications with service lines” Journal of Systems and Software, Vol.91, pp.48-62.2014.
[28]. Wonil Kim, Joo Hwan Lee, Chuleui Hong, Changhee Han, Bongshik Jang, “An innovative method for data and software integration in SaaS" Computers and Mathematics with Applications, Vol.64, No.5, pp.1252-1258.2012.
[29]. Luis Rodero-Merino, Lúis M. Vaquero, Eddy Caron, Adrian Muresan, Frédéric Desprez, “Building safe PaaS clouds: A survey on security in multitenant software platforms” Computers and Security, Vol.31, No.1, pp.96-108.2012.
attacks for database systems” Theoretical Computer Science, Vol.767, pp.51-72,2019.

68. Scott Paquet, Paul T. Jaeger, Susan C. Wilson, “Identifying the security risks associated with governmental use of cloud computing” Government Information Quarterly, Vol.27, No. 3, pp.245-253,2010.

69. Nalegaaev.S.S, Petrov.N.V, “Simple Criteria to Determine the Set of Key Parameters of the DRPE Method by a Brute-force Attack” Physics Procedia, Vol.73, pp.281-286,2015.

70. Jung-Sik Cho, Sung-Soo Yeo, Sung Kwon Kim, “Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value” Computer Communications, Vol.34, No.3, pp.391-397,2011.

71. Alex X. Liu, Jason M. Kovaec, Mohamed G. Gouda, “A secure cookie scheme” Computer Networks, Vol.56, No.6, pp.1723-1730,2012.

72. Selvanamini, Pradeep Kumar Arya, “Credentialed Based Authentication Approach for Dynamic Group in Cloud Environment” Procedia Computer Science, Vol.48, pp.166-172,2015.

73. Indu, P. M. Rubesh Anand, Vidhyacharan Bhaskar, “Identity and access management in cloud environment: Mechanisms and challenges” Engineering Science and Technology, an International Journal, Vol.21, No.7, pp.574-588,2018.

74. Zhiheng Xu, Quanyan Zhu, “A Secure Data Assimilation for Large-Scale Sensor Networks Using an Untrusted Cloud” IFAC-Papers OnLine, Vol.50, No.1, pp.2609-2614,2017.

75. Yuiaob Wang, Junhao Wen, Xbin Wang, Wei Zhou, “Cloud service evaluation model based on trust and privacy-aware” Optik, Vol.134, pp.269-279,2017.

76. Antonio Rico, Manuel Nogueria, José Luis Garrido, Kawtar Benghazii, Lawrence Chung, “Supporting Agile Software Development and Deployment in the Cloud: A Multitenant, Multitagret Architecture” Agile Software Architecture, Vol.20, pp.269-288,2014.

77. Luis Rodero-Merino, Luis M. Vaquero, Eddy Caron, Adrian Muresan, Frédéric Desprez, “Building safe PaaS clouds: a survey on security in multitenant software platforms” Computers and Security, Vol.31, No.1, pp.96-108,2012.

78. Mahmoudi, “Cloud and Mobile Cloud Architecture, Security and Safety” Handbook of System Safety and Security, pp.199-223,2017.

79. Saru Kumari, Xiong Li, Fan Wu, Ashok Kumar Das, Jian Shen, “Design of a provably secure biometrics-based multi-cloud-server authentication scheme” Future Generation Computer Systems, Vol.68, pp.320-330,2017.

80. Indu I., Rubesh Anand P.M., Vidhyacharan Bhaskar, “Encrypted token-based authentication with adapted SAML technology for cloud web services” Journal of Network and Computer Applications, Vol.99, pp.131-145,2017.

81. Jui-Ting Chung, Chuan-Ming Li, Tzonelih Hwang, “All-in-one group-oriented cryptosystem based on bilinear pairing” Information Sciences, Vol.177, No.24, pp.5651-5663,2007.

82. Cheng Guo, Ningji Luo, Md Zakirul Alam Bhuiyan, Yingmo Jie, Muhammad Alam, “Key-aggregation authentication cryptosystem for data sharing in dynamic cloud storage” Future Generation Computer Systems, Vol.84, pp.190-199,2018.

83. Zhiwei Wang, “Provably secure key-aggregate cryptosystems with auxiliary inputs for data sharing on the cloud” Future Generation Computer Systems, Vol.93, pp.770-776,2019.

84. Chun-Ta Li, Dong-Her Shih, Chun-Cheng Wang, “Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems” Computer Methods and Programs in Biomedicine, Vol.157, pp.191-203,2018.

85. Tao Xiang, Jia Hu, Jianglin Sun, “Outsourcing chaotic selective image encryption to the cloud with steganography” Digital Signal Processing, Vol.43, pp.287-307,2015.

86. Mamta Jain, Saroj Kumar Lenka, Sunil Kumar Vasishta (2016), “Adaptive circular queue image steganography with RSA cryptosystem” Perspectives in Science, Vol.8, pp.417-420,2016.

87. Praveen Kumar P, Syam Kumar P, Alphonse P.J.A., “Attribute based encryption in cloud computing: A survey, gap analysis, and future directions” Journal of Network and Computer Applications, Vol.108, pp.37-52,2018.

88. Qian He, Ning Zhang, Yongzhuan Wei, Yan Zhang, “Lightweight attribute-based encryption scheme for mobile cloud assisted cyber-physical systems” Computer Networks, Vol.140, pp.163-173,2018.

89. Jing Li, Qihong Yu, Yuchen Zhang, Jian Shen, “Key-policy attribute-based encryption against continual auxiliary input leakage” Information Sciences, Vol.470, pp.175-188,2019.

90. Malluhi Q.M, A. Shikfa, V. D. Tran, V. C. Trinh, “Decentralized ciphertext-policy attribute-based encryption schemes for lightweight devices” Computer Communications, Vol.145, pp.113-125,2019.

91. Baodong Qin, Qinglan Zhao, Dong Zheng, Hui Cui, “(Dual) server-aided revocation attribute-based encryption with decryption key exposure resistance” Information Sciences, Vol.490, pp.74-92,2019.

92. Boaz Tsaban , “Fast generators for the Diffie-Hellman key agreement protocol and malicious standards” Information Processing Letters, Vol.99, No.431, pp.145-148,2006.

93. Mbarek Marwan, Ali Kartisi, Hassan Ouahmane, “Security Enhancement in Healthcare Cloud using Machine Learning” Procedia Computer Science, Vol.127, pp.388-397,2018.

94. Saurabh Dey, Qiang Ye, Srinivas Sampalli, “A machine learning based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks” Information Fusion, Vol.49, pp.205-215,2019.

95. Gautam M. Borkar, Leena H. Patil, Dilip Dalgade, Ankush Hukte, “A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept” Sustainable Computing: Informatics and Systems, Vol.23, pp.120-135,2019.

96. Fangjun Kuang, Weihong Xu, Siyang Zhang, “A novel hybrid KPCA and SVM with GA model for intrusion detection” Applied Soft Computing, Vol.18, pp.178-184,2014.

97. Wang Chao, Wang Junzheng, “Cloud-service decision tree classification for cloud platform” Cognitive Systems Research, Vol.52, pp.234-239,2018.

98. Weizhi Meng, Wenjuan Li, Yang Xiang, Kim-Kwang Raymond Choo, “A bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks” Journal of Network and Computer Applications, Vol.78, pp.162-169,2017.

99. Varsha R. Mouli, K. P. Jevitha, “Web Services Attacks and Security- A Systematic Literature Review” Procedia Computer Science, Vol.93, pp.870-877,2016.

100. Peng Li, Zhikui Chen, Laurence T. Yang, Liang Zhao, Qingchen Zhang, “A privacy-preserving high-order neuro-fuzzy c-means algorithm with cloud computing” Neurocomputing, Vol.256, pp.82-97,2017.

101. Thanachai, Santiprabhob, Pratit, “Fuzzy Intrusion Detection System” AU Journal of Technology. Vol.6, No.2, pp.109-114,2002.

102. Dipak Kumar Jana, Ramkrishna Ghosh, “Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security” Journal of Information Security and Applications, Vol.40, pp.173-182,2018.

103. Lu Zhou, Youwen Zhu, Kim-Kwang Raymond Choo, “Efficiently and securely harnessing cloud to solve linear regression and other matrix operations” Future Generation Computer Systems, Vol.81, pp.404-413,2018.

104. Xinyu Lei, Xiaofeng Liao, Tingwen Huang, Feno Hermiain, “Achieving security, robust cheating resistance, and high-efficiency for TTP outsourcing of large matrix multiplication computation to a malicious cloud” Information Sciences, Vol.28, pp.205-217,2014.
Advances in Computing, Communication, Automation and Biomedical Technology

[105]. Salman Iqbal, Miss Laiha Mat Kiah, Babak Daghlish, Muzammil Hussain, Kim-Kwang Raymond Choo, “On cloud security attacks: A taxonomy and intrusion detection and prevention as a service’ Journal of Network and Computer Applications, Vol.74, pp.98-120,2016.

[106]. Rajendra Patil, Harsha Dudeja, Chirag M., “Designing an efficient security framework for detecting intrusions in virtual network of cloud computing” Computers & Security, Vol.85, pp.402-422,2019.

[107]. Henrique Yoshikazu Shishido, Júlio Cezar Estrela, Claudio Fabiano Motta Toledo, Marcio Silva Arantes, “Genetic-based algorithms applied to a workflow scheduling algorithm with security and deadline constraints in clouds” Computers & Electrical Engineering, Vol.69, pp.378-394,2018.

[108]. Rahulamathavan, Rahul, Phan, Raphael, Veluru, Suresh, Cumanan, Kanapathippillai, Rajarajan, Muttukrishnan, “Privacy-preserving multi-class support vector machine for outsourcing the data classification in cloud” IEEE Transactions on Dependable and Secure Computing, Vol.11, No.5, pp.467-479,2013.

[109]. Appavu alias Balamurugan, Ramassamy Rajaram, “Effective solution for unhandled exception in decision tree induction algorithms” Expert Systems with Applications, Vol.36, No.10, pp.12112-12119,2009.

[110]. Mohammad Amin Adibi, “Single and multiple outputs decision tree classification using bi-level discrete-continues genetic algorithm” Pattern Recognition Letters, Vol.128, pp.190-196,2019.

[111]. Abdulatif Alabulatif, Heshan Kumarage, Ibrahim Khalil, Xun Yi, “Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption” Journal of Computer and System Sciences, Vol.90, pp.28-45,2017.

[112]. Katherapaka Sudhakar, M.A.H. Farquad, Narshimha, “Effective convolution method for privacy preserving in cloud over big data using map reduce framework” IET Software, Vol.13, No.3, pp.187-194,2019.

[113]. Wei Wu, Jian Liu, Hong Rong, Huimei Wang, Ming Xian, “Efficient k-Nearest Neighbor Classification Over Semantically Secure Hybrid Encrypted Cloud Database” IEEE Access, Vol.6, pp.41771-41784,2018.

[114]. Nalini Subramanian, Andrews Jeyaraj, “Recent security challenges in cloud computing” Computers & Electrical Engineering, Vol.71, pp.28-42,2018.

[115]. Zouhair Chiba, Noreeddine Abghour, Khalid Moussaid, Amina El Omri, Mohamed Rida, “A novel architecture combined with optimal parameters for back propagation neural networks applied to anomaly network intrusion detection” Computers & Security, Volume 75, pp.36-58,2018.

[116]. Zouhair Chiba, Noreeddine Abghour, Khalid Moussaid, Amina El omri, Mohamed Rida, “Intelligent approach to build a Deep Neural Network based IDS for cloud environment using combination of machine learning algorithms” Computers and Security, Vol.86, pp.301-317,2019.

[117]. Anindita Pratap Singh, Syam Kumar Pasupuleti, “Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud Computing” Procedia Computer Science, Vol.93, pp.751-759,2016.

[118]. Esma Yildirim, Jangyoung Kim, Tefvik Kosar (2013), “Modeling throughput sampling size for a cloud-hosted data scheduling and optimization service” Future Generation Computer Systems, Vol.29, No.7, pp.1795-1807,2013.

[119]. Ousmane Diallo, Ouarda Zedadra, Antonio Guerrieri, Nicolas Jouandeau, Giandomenico Spezzano, Giancarlo Fortino, “Swarm intelligence-based algorithms within IoT-based systems: A review” Journal of Parallel and Distributed Computing, Vol.122, pp.173-187,2018.

[121]. Yuming Xu, Kenli Li, Ligang He, Tung Khac Truong, “A DAG scheduling scheme on heterogeneous computing systems using double molecular structure-based chemical reaction optimization” Journal of Parallel and Distributed Computing, Vol.73, No.9, pp.1306-1322,2013.

[122]. Farzaneh Abazari, Morteza Analoui, Hassan Takabi, Song Fu, “Multi-objective workflow scheduling in cloud computing based on heuristic algorithm” Simulation Modelling Practice and Theory, Vol.93, pp.119-132,2019.

[123]. Manwar Hashim Ewana, Salma Hamdy Mohammed, El-Sayed M. El-Horbaty, “Hybrid Algorithm for Resource Provisioning of Multi-tier Cloud Computing” Procedia Computer Science, Vol.65, pp.682-690,2015.

[124]. Weiping Ding, Zhihun Guan, Quan Shi, Jiandong Wang, “A more efficient attribute self-adaptive co-evolutionary reduction algorithm by combining quantum elitist frogs and cloud model operators” Information Sciences, Vol.293, pp.214-234,2015.

[125]. Chunlin Li, Jing Zhang, Yi Chen, Youlong Luo, “Data prefetching and file synchronization for performance optimization in Hadoop-based hybrid cloud” Journal of Systems and Software, Vol.151, pp.133-149,2019.

[126]. Hamdi Hassen, Maher Khemakhem, “Large Distributed Arabic Handwriting Recognition System based on the Combination of FastDTW Algorithm and Map-reduce Programming Model via Cloud Computing Technologies” AASRI Procedia, Vol.52, pp.156-163,2013.

[127]. Jorge L. Reyes-Ortiz, Luca Oneto, Davide Anguita, “Big Data Analytics in the Cloud: Spark on Hadoop vs MPI/OpenMP on Beowulf” Procedia Computer Science, Vol.53, pp.121-130,2015.

[128]. Henrique Yoshikazu Shishido, Júlio Cezar Estrela, Claudio Fabiano Motta Toledo, Marcio Silva Arantes (2018), “Genetic-based algorithms applied to a workflow scheduling algorithm with security and deadline constraints in clouds” Computers & Electrical Engineering, Vol.69, pp.378-394,2018.

[129]. Abdullah Konak, Sadak Kulturel-Konak, Lawrence V. Snyder, “A Game-Theoretic Genetic Algorithm for the reliable server assignment problem under attacks” Computers and Industrial Engineering, Vol.85, pp.73-85,2015.

[130]. Yingfeng Zhang, Jin Wang, Yang Liu, “Game theory based real-time multi-objective flexible job shop scheduling considering environmental impact” Journal of Cleaner Production, Vol.167, pp.665-679,2017.

[131]. Mariestella Oliveira Santos, Sadao Massago, Bernardo Almada-Lobo, “Infeasibility handling in genetic algorithm using nested domains for production planning” Computers and Operations Research, Vol.37, No.6, pp.1113-1122,2010.

[132]. Najme Mansouri, Behnam Mohammad Hasani Zade, Mohammad Masoud Javidi, “Hybrid task scheduling strategy for cloud computing by modified particle swarm optimization and fuzzy theory” Computers and Industrial Engineering, Vol.130, pp.597-633,2019.

[133]. Shabeera, Madihah Kumar, Sameera, Salam, Murali Krishnan, “Optimizing VM allocation and data placement for data-intensive applications in cloud using ACO metaheuristic algorithm” Engineering Science and Technology, an International Journal, Vol.20, No.2, pp.616-628,2017.

[134]. Yongqiang Gao, Haibing Guan, Zhengwei Qi, Yang Hou, Liang Liu, “A multi-objective ant colony system algorithm for virtual machine placement in cloud computing” Journal of Computer and System Sciences, Vol.79, No.8, pp.1230-1242,2013.

[135]. Bahram Hajimirzaei, Nima Jafari Navimipour, “Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm” ICT Express, Vol.5, No.1, pp.56-59,2019.

[136]. Javid Taheri, Yong Choon Lee, Albert Y. Zomaya, Howard Jay Siegel, “A Bee Colony based optimization approach for simultaneous job scheduling and data replication in grid
environments” Computers and Operations Research, Vol.40, No.6, pp.1564-1578,2013.

[137]. Navneet Kaur, Sarbjeet Singh, “A Budget-constrained Time and Reliability Optimization BAT Algorithm for Scheduling Workflow Applications in Clouds” Procedia Computer Science, Vol.98, pp.199-204,2016.

[138]. Mhamed Zineddine, “Optimizing security and quality of service in a real-time operating system using multi-objective Bat algorithm” Future Generation Computer Systems, Vol.87, pp.102-114,2018.

[139]. Mhamed Zineddine, “Vulnerabilities and mitigation techniques tuning in the cloud: A cost and vulnerabilities coverage optimization approach using Cuckoo search algorithm with Lévy flights” Computers and Security, Vol.48, pp.1-18,2015.

[140]. Massimo Ficco, Beniamino Di Martino, Roberto Pietrantuono, Stefano Russo (2017), “Optimized task allocation on private cloud for hybrid simulation of large-scale critical systems” Future Generation Computer Systems, Vol.74, pp.104-118,2017.

[141]. Sadip Midya, Asmita Roy, Koushik Majumder, Santanu Phadikar, “Multi-objective optimization technique for resource allocation and task scheduling in vehicular cloud architecture: A hybrid adaptive nature inspired approach” Journal of Network and Computer Applications, Vol.103, pp.58-84,2018.

[142]. Shuai Ding, Chengyi Xia, Chengjiang Wang, Desheng Wu, Youtao Zhang, “Multi-objective optimization based ranking prediction for cloud service recommendation” Decision Support Systems, Vol.101, pp.106-114,2017.

[143]. IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks,” in IEEE Std 802.15.6-2012, vol., no., pp.1-271, 29 Feb. 2012, doi: 10.1109/IEEESTD.2012.6161600.