International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Teaching Network Security with IP Darkspace Data

N. Pradeep[1], Dr. A. Jayachandran[2]

[1]PG Scholar, Department of M.Sc (Software Engineering), PSN College of Engineering & Technology, Tirunelveli, Tamilnadu, India

[2] Research Supervisor, Department of M.Sc (Software Engineering), PSN College of Engineering & Technology, Tirunelveli, Tamilnadu, India

ABSTRACT

The fifth generation (5G) mobile networks are envisioned to support the deluge of data traffic with reduced energy consumption and improved quality of service (QoS) provision. To this end, key enabling technologies, such as heterogeneous networks (HetNets), massive multiple-input multiple-output (MIMO), and millimeter wave (mmWave) techniques, have been identified to bring 5G to fruition. Regardless of the technology adopted, a user association mechanism is needed to determine whether a user is associated with a particular base station (BS) before data transmission commences. User association playsa pivotal role in enhancing the load balancing, the spectrum efficiency, and the energy efficiency of networks. The emerging 5Gnetworks introduce numerous challenges and opportunities for the design of sophisticated user association mechanisms. Hence, substantial research efforts are dedicated to the issues of user association in HetNets, massive MIMO networks, mmWave networks, and energy harvesting networks. We introduce taxonomy as framework for systematically studying the existing user association algorithms. Based on the proposed taxonomy, we then proceedto present an extensive overview of the state-of-the-art in user association algorithms conceived for HetNets, massive MIMO,mmWave, and energy harvesting networks. Finally, we summarize the challenges as well as opportunities of user association in 5G and provide design guidelines and potential solutions for sophisticated user association mechanisms.

Keywords : PPP 5G-Public Private Partnership**,** Zero-Forcing, Cumulative Distribution Function, Capital Expenditure, Binomial Point Process, Capacity and Coverage Optimization.

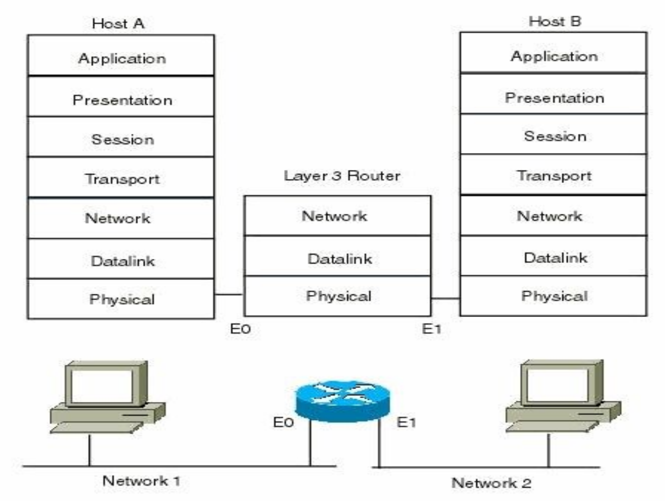
I. INTRODUCTION

A computer network or data network is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices exchange data with each other using data link. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, and serversas well as networking hardware. Two such devices can be said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other. Computer networks differ in the transmission medium used to carry their signals,communications protocolsto organize network traffic, the network's size,topologyand organizational intent.

Computer networks support an enormous number of applications and services such as access to the World Wide Web,digital video,digital audio, shared use ofapplication and storage servers,printers, andfax machines, and use of emailand instant messaging applications as well as many others. In most cases, application-specific communications protocols are layered (i.e. carried as payload) over other more general communications protocols.

A computer network facilitates interpersonal communications allowing users to communicate efficiently and easily via various means: email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing. Providing access to information on shared storage devices is an important feature of many networks. A network allows sharing of files, data, and other types of information giving authorized users the ability to access information stored on other computers on the network. A network allows sharing of network and computing resources. Users may access and use resources provided by devices on the network, such as printing a document on a shared network printer. Distributed computing uses computing resources across a network to accomplish tasks. A computer network may be used bycomputer crackersto deploycomputer virusesorcomputerworm son devices connected to the network, or to prevent these devices from accessing the network via adenial of serviceattack.



Legitimate user through a door and this is referred to as "tailgating". Often the legitimate user will hold the door for the intruder. This risk can be minimized through security awareness training of the user population, or more active means such as turnstiles. In very high security applications this risk is minimized by using a sally port, sometimes called a security vestibule or mantrap, where operator intervention is required presumably to assure valid identification.

II. METHODS AND MATERIAL

A. Literature Survey

Existing work on access control in cloud are centralized in nature. All other schemes use attribute based encryption. The scheme uses a symmetric key approach and does not support authentication. The other drawback was that an user can create and store a file and other users can only read the file. Write access was not permitted to users other than the creator. could be supported:

1) HaaS: Hardware as a Service:

Hardware as a Service was proposed possibly at 2006. As an outgrowth of rapid advances in hardware virtualization, IT automation and usage metering and pricing, users could buy IT hardware - or even an entire data center/computer center - as a pay-as-you-go subscription service. The HaaS could be flexible, scalable and manageable to meet your needs.

2) SaaS: Software as a Service:

Software or application is hosted as a service and provided

to customers across the Internet, which excludes the requirement to install and run the application on the customer's local computer. SaaS therefore amends the customer's headache of software maintenance, and decreases the expense of software purchases by on demand pricing.

3) DaaS: Data as a Service:

Data in various formats, from various sources, could be accessed via services to users on the network. Users could, for example, manipulate remote data just like operate on local disk; or access data in a semantic way on the Internet.

Nelson Gonzalez, Charles Miers, Fernando Redígolo, Tereza Carvalho, Marcos Simplicio, Mats Näslundy and Makan Pourzandi in their research paper, "An quantitative analysis of current security concerns and solutions for cloud computing", in Springer 2012 - Aiming to organize the information related to cloud security have identify the main problems in the area and grouped them into a model composed of seven categories: network security, interfaces, data security, virtualization, governance, compliance and legal issues.

Glee et al [4]. To address these problems, our main scheme for ensuring cloud data storage is presented.

The first part of the section is devoted to a review of basic tools from coding theory that is needed in our scheme for file distribution across cloud servers. Then, the homomorphic token is introduced. The token computation function we are considering belongs to a family of universal hash function, chosen to preserve the homomorphic properties, which can be perfectly integrated with the verification of erasure-coded data . Subsequently, it is shown how to derive a challenge response protocol for verifying the storage correctness as well as identifying misbehaving servers. The procedure for file retrieval and error recovery based on erasure correcting code is also outlined. Finally, we describe how to extend our scheme to third party auditing with only slight modification of the main design.

S. Kamara and K. Lauter, Cryptographic Cloud Storage, [3] To support lazy-revocation and hierarchies, Key to Compute uses scheme that is based on Key-Policy Attribute-Based encryption scheme. A general cryptographic library is developed and released it as an independent open source project .
Simplicity and extendability are two major design goals of K2C framework. K2C framework is independent of any specific cloud provider. It has two simple interfaces which abstract away the details of the cloud providers: IDataStore and IMetadataDirectory. A new cloud service provider can be supported easily by implementing these interfaces. Out of the box, framework comes with a data store driver for Amazon S3 and a meta-data directory driver which uses Amazon Simple. To make it easier for the developers to learn and use our framework, we expose its services through a set of APIs which are very similar to the Java APIs for accessing the file system. Lazy revocation was first introduced in Cephues to eliminate re-encryption required for each revocation at the cost of slightly lowered security. Lazy revocation, which is widely being used in recent cryptographic file systems, requires a key-updating scheme to support key regression.

They describe several scenarios in which IBC simplifies the current grid solutions, like the elimination of the use of certificate, simple proxy generation, easy revocation of proxy certificates and the savings of bandwidth by using the pairing based approach proposed by Boneh and Franklin. In the same way, Li et al propose to use IBC as an alternative to the SSL authentication protocol in a cloud environment. However, these schemes still suffer from the needed trust hierarchy to ensure a secure working system.

H. Li, Y. Dai, L. Tian, and H. Yang, [5] Identity-Based Authentication for Cloud Computing,Cloud computing is a style of computing in which dynamically scalable and commonly virtualized resources are provided as a service over the Internet. This paper, first presents a novel Hierarchical Architecture for Cloud Computing (HACC). Then, Identity-Based Encryption (IBE) and Identity-Based Signature (IBS) for HACC are proposed. Finally, an Authentication Protocol for Cloud Computing is presented. Performance analysis indicates that APCC is more efficient and lightweight than SSL Authentication Protocol (SAP), especially for the user side. This aligns well with the idea of cloud computing to allow the users with a platform of limited performance to outsource their computational tasks to more powerful servers. Cloud computing provides a number of advantages that include economies of scale, dynamic provisioning, increased flexibility and low capital expenditures; it also introduces a range of new security risks. IBE-based systems do not require certificate management, eliminating the need for certificate lookups and complex certificate revocation schemes.

B. Application of Neural Network In Intrusion Detection

Nature provides us with information processing problems can be divided into two categories: structural and non structural problems. The former can be used mathematical language clearly and strictly described and can be solve the problem of algorithm formula, and mapped into a computer program, then by the computer one by one to execute the program of instruction, when given different initial values, was calculated with a computer the corresponding results, because of this, von Neumann computer in solving structural problems far exceeds the ability of human beings. But for non-structural problems, it is difficult for people to translate their own understanding into machine instructions, or only to a very rough. So the computer is very far away from human ability when dealing with the artificial intelligence and pattern recognition of image processing and scene analysis, speech recognition and understanding, intelligent robot control and so on.

Artificial neural network is proposed on the research achievements of modern neural based and mainly focus on the human brain microstructure, trying to from the physical structure of the brain up study of human wisdom and form, it is by a large number of similar to neurons of simple processing units are extensively interconnected and complex network giant system, reflecting the brain function of some functions, but not nervous system the real

C. Artificial Neural Network Model

A neural network model based on different angles and background can be defined by multiple, Kohonen had using the artificial neural network is a general and abstract definition: artificial neural network (ANN) is by some simple (usually adaptive element and its hierarchical organization of massively parallel connection structure of the network. It aims to deal with real world objects in biological neural systems in the same manner. The artificial neural network model is determined by three factors: the network topology, the characteristics of neurons, learning or training rules. Although the structure and function of each neuron is very simple, the behavior of the network model which is composed of a large number of neurons is more and more diverse. Because the neural network is nonlinear, so the overall nature is not equal to the simple addition of the unit, which is one of the basic characteristics of the human brain. In addition, there is considerable robustness and fault tolerance the NN, NN has a large number of computing nodes, each node and by the weight coefficient and a lot of other nodes are connected, information is to distribution of stored in the weight function, when between a few nodes or node connection damage, as for the performance of the entire network caused catastrophic effects.

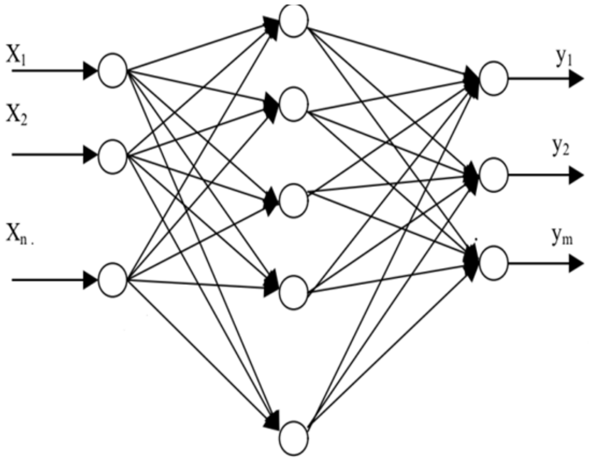


Figure 1. Three layer feed-forward neural network structure

$$\underset{i}{f(net)} = \frac{1}{1 + e - neti}$$

Output layer of neurons in the input information and the formula for calculating the hidden layer of the input formula similar to; output layer of neurons in the output formula similar to the hidden layer of neurons in the output formula; output layer this paper take sigmoid function as the excitation function for the output layer. Now there are few studies on the application of neural network in intrusion detection, which can be used to solve the problems encountered by other intrusion detection methods. The existing anomaly detection system is a very difficult problem is how to correctly identify those past.

The Data are accessed in centralized form on the basis of key distributed center. Key distributed center does not support for authentication. A single failure of KDC can affect the maximum number of data in cloud storage. It is most difficult to maintain the large number of data in cloud for centralized form. Accountability of clouds is a very challenging task and involves technical issues and law enforcement. Neither clouds nor users should deny any operations performed or requested. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. we propose our privacy preserving authenticated access control scheme.

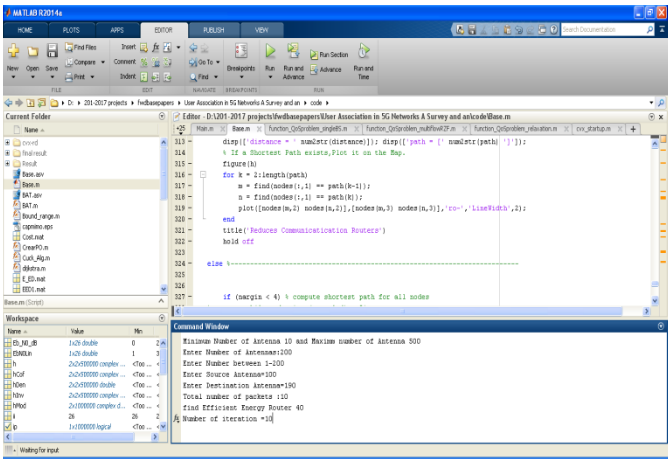
D. Proposed System

Maintaining the large number of data in cloud, decentralized access control approaches is proposed. Involving distribution of secret keys and attributed of all users. Authentication access control only allows the user for reading purpose. Accessing the data by user only satisfying the access policy and authentication. Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. Authentication of users who store and modify their data on the cloud. The identity of the user is protected from the cloud during authentication.

Revoked users cannot access data after they have been revoked. The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information. The protocol supports multiple read and writes on the data.

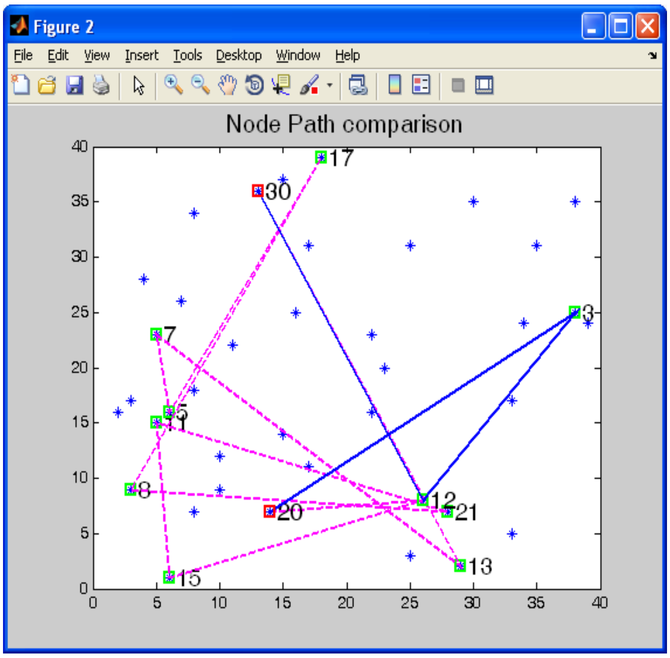
III. EXPERIMENTAL RESULTS

The Implementation Results can be shown as figure below

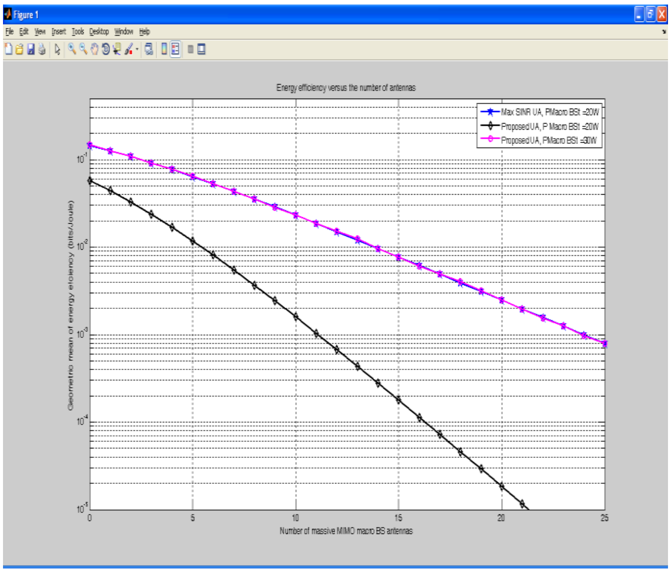

MATLAB R2014a
HOME
PLOTS
APPS
EDITOR
PUBLISH
VIEW
Run Section
Advance
Breakpoints
Run
Run and Advance
Run and Time
Go To
Find
Current Folder
Workspace
Editor - D:\201-2017 projects\fwdbasepapers\User Association in 5G Networks A Survey and an\code\Base.m
Main.m
Base.m
function_QoSproblem_singleBS.m
function_QoSproblem_multiflowRZF.m
function_QoSproblem_relaxation.m
cvx_startup.m
Command Window

```
        disp(['distance = ' num2str(distance)]); disp(['path = [' num2str(path) ']']);
        % If a Shortest Path exists,Plot it on the Map.
        figure(h)
        for k = 2:length(path)
            m = find(nodes(:,1) == path(k-1));
            n = find(nodes(:,1) == path(k));
            plot([nodes(m,2) nodes(n,2)],[nodes(m,3) nodes(n,3)],'ro-','LineWidth',2);
        end
        title('Reduces Communicatication Routers')
        hold off

    else %------------------------------------------------------------------------


        if (nargin < 4) % compute shortest path for all nodes
```

```
Minimum Number of Antenna 10 and Maximm number of Antenna 500
Enter Number of Antennas:200
Enter Number between 1-200
Enter Source Antenna=100
Enter Destination Antenna=190
Total number of packets :10
find Efficient Energy Router 40
Number of iteration =10
```



The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information. The protocol supports multiple read and writes on the data stored in the cloud. The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud. Access control with authentication is provided on the basis of attribute based access control.



IV. CONCLUSION

The pertinent user association algorithms designed for HetNets, massive MIMO networks, mmWave scenarios and energy harvesting networks have been surveyed, which constitute four of the most salient enabling technologies envisioned for future 5G networks. In order to systematically survey the existing user association algorithms, we have presented a related taxonomy. Within each of the networks considered, we have highlighted the inherent features of the corresponding 5G enabling technology, which have a substantial impact on the user association decision, and then categorized the state-of-threat user association algorithms. However, given the intricate and perpetually evolving 5G network conditions, the related research relying on sophisticated machine learning techniques is still in its infancy.

V. REFERENCES

[1]. D. F. Ferraiolo and D.R. Kuhn, "Role-Based A Cisco, "Cisco visual networking index: Global mobile data traffic forecast update 2014–2019," White paper, Feb. 2015.

[2]. FP7 European Project. Evolving Mobile Internet With Innovative Terminal-to-Terminal Offloading Technologies (MOTO) [Online]. Available: http://www.fp7-moto.eu/

[3]. J. Wu, Y. Zhang, M. Zukerman, and E. Yung, "Energy-efficient base stations sleep-mode techniques in green cellular networks: A survey," IEEE Commun. Surveys Tuts., vol. 17, no. 2, pp. 803–826, Second quart. 2015.

[4]. M. Haddad, P. Wiecek, E. Altman, and H. Sidi, "A game theoretic approach for the association problem in two-tier HetNets," in Proc. 25thInt. TeletrafficCongr. (ITC), Sep. 2013, pp. 1–9.

[5]. W. Saad, Z. Han, R. Zheng, M. Debbah, and H. Poor, "A college admissions game for uplink user association in wireless small cell networks," in Proc. IEEE INFOCOM, Apr. 2014, pp. 1096–1104.

[6]. M. Hong and Z.-Q. Luo, "Distributed linear precoder optimization and base station selection for an uplink heterogeneous network," IEEE Trans. Signal Process., vol. 61, no. 12, pp. 3214–3228, Jun. 2013.

[7]. D. Zhao, C. Huang, Y. Chen, F. Alsaadi, and S. Cui, "Resource allocation for multiple access channel with conferencing links and shared renewable energy sources," IEEE J. Sel. Areas Commun., vol. 33, no. 3, pp. 423–437, Mar. 2015.

[8]. D. Liu, Y. Chen, K. K. Chai, and T. Zhang, "Optimal user association for delay-power tradeoffs in HetNets with hybrid energy sources," in Proc.IEEE 25nd Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC), Sep. 2014, pp. 1857–1861.

[9]. T. Han and N. Ansari, "On optimizing green energy utilization for cellular networks with hybrid energy supplies," IEEE Trans. WirelessCommun., vol. 12, no. 8, pp. 3872–3882, Aug. 2013.

[10]. Y. L. Che, L. Duan, and R. Zhang, "Spatial throughput maximization of wireless powered communication networks," arXiv preprint arXiv:1409.3107, Oct. 2014.