Parichay: Maharaja Surajmal Institute Journal of Applied Research

Intrusion Detection Techniques for Mobile Cloud Computing in Heterogenous 5G Technologies

Harjender Singh*

Abstract: ***As the importance of distributed computers is rapidly growing, they are becoming the target of more and more crime. Intrusion may be defined as the set of attempts to compromise computer network security. Besides the several security services, Intrusion Detection System/Techniques are taken into point that strengthen the system security and is more powerful in preventing internal and external attacks. This technique is considered to be very efficient in preventing wireless communication in Fifth Generation. In this paper we will discuss what Mobile Cloud Computing is and various Intrusion Detection Techniques for mobile computing along with challenges faced by each technique.***

Keywords: ***Intrusion, Mobile Cloud Computing, Intrusion Detection System/Techniques.***

1. INTRODUCTION

The latest fast growth of advanced mobile technologies led to a great advantage in the development of mobile cloud computing (MMC). Mobile devices performance has enhanced by incorporating three technologies in which the first one to be involved is cloud computing, second is mobile internet and third is mobile computing in which choosing MCC has become main advantage.

Taking into consideration, Fifth Generation (5G) background in the coming time, MCC will achieve greater class performances in unloading computation by relocating data storage and processing data to the cloud so that the abilities of the mobile devices can be enhanced [4-7] by the cause of improved bandwidth. Though, lot of provocations will be faced by advanced wireless networks [8, 9], that has been investigated from different aspect by earlier research [10]. Out of which one of the provocations is that controlling risk from intrusions is not easy because of managing tool limitations, mutual interferences between signal cells, high efficiency wireless communications, intentional attacks and improper user authentications. The intrusions are concealed by attackers with the help of enhanced networking speed.

The paper shows safety concerns in MCC and combines latest attainments all together in intrusion detection abilities so that the approaches can be found which can successfully deploy the rise in heterogeneous 5G. As Intrusion Detection System (IDS) is a vital authority that has been related with various techniques. As each technique has different property therefore each observation process has both prevalence and restrictions. The major benefactions of this paper are bifold:

- It allocates 5G users of future and developers with an analytical efficient model to attain safe data communication.
- It analysis and integrates all critical safety concerns in MCC from a technical aspect.

2. MOBILE CLOUD COMPUTING TERMINOLOGY IN FIFTH GENERATION

A. MOBILE CLOUD COMPUTING

To extend cloud to the edge of the networks, one of the cloud service models, MOBILE CLOUD COMPUTING is fast emerging. It consists of various mobile devices that are useful for many users. A prediction was made by Gartner that by 2013, PCs will be overtaken by mobile phones as the most common web access devices, worldwide [1]. Mobile Cloud Computing mainly tells how the resources of cloud can be best utilized by smart phones to reduce its consumption of energy. And a particular task can be executed either on mobile device or can be sent to cloud. Overhead tradeoffs between communication and computation, decides where to execute the task. One of the most important features is that the data processing and data storage are migrated from mobile devices to cloud. With this feature, to support applications running in cloud MCC model is designed that offers high level centralized functions. If we talk about security in MCC model, the security problems can be addressed by threat assessment from three technologies- Mobile Internet, Cloud Computing and Mobile Computing [2]. This model also helps in reducing obstacles that are related to security (reliability and privacy), performance and environment.

1. MOBILE COMPUTING

To enable devices that are portable, to access the services available on the web, a platform known as Mobile Computing is developed that is supported by wireless networks. It is a

*Asst. Professor, Maharaja Surajmal Institute (GGSIPU), New Delhi; singh.harjender@gmail.com

technology in which without being connected to a fixed physical link, we can transmit data, video and voice via any wireless device. It involves the following:

a. *Mobile Hardware:* To receive and access the service of mobility, Mobile devices or components comes in this category such as, tablet PCs, portable laptops, smartphones, etc. These devices are capable of sending and receiving signals at the same time.

b. *Mobile Communication:* To ensure that seamless and reliable communication goes on, mobile communication is an infrastructure that is put in place for the same. For example, services, portal, protocols and bandwidth necessary to support the services. It ensures that the other systems that offers the same service, does not collide.

c. *Mobile Software:* It is the actual program that runs on the mobile hardware. It is the operating system of appliance. It deals with the demands and characteristics of mobile applications. It is the most essential component used to operate mobile devices.

It is useful in reducing application's development time. When communication takes place, it also faces threats. For example, one of the threats is when using virtual private network, the wireless communication can be easily invaded because of interconnection of various networks. Authentication and encryption methods are used for security in mobile computing for virtual private network access.

2. MOBILE INTERNET

The method of accessing browser based Internet services from mobile devices, such as smartphones, through wireless networks is referred to as mobile internet. It is a technology derived from development of wireless networks. Some recent technologies that are active, includes: Third Generation (3G), Mobile Commerce (M-commerce), WiFi and long term evolution. The future asset for mobile internet is 5G. The central idea of mobile internet is to connect two communicators that support Web services, via wireless network. Web services may be defined as any software that makes itself available on internet and uses a standardized messaging system known as XML. It can also be defined as consolidation of web applications by using Simple Object Access Protocol, Extensible Markup Language, Web Services Description Language and Universal Description, Discovery and Integration. The security criteria and requirements may vary in mobile internet. Therefore, they often address service layer objects such as application, platform and infrastructure layer. It doesn't matter which layer is choose, wireless network itself always faces threats from intrusion.

3. BEHIND CLOUD COMPUTING

Cloud computing have some technologies that are similar to the deployments or service types[10, 11].Basically, there are three technologies that are adopting the cloud computing with the Mass Distributed Storage(MDS) virtualization and the technology that are under the Parallel Programming Model(PPM)[12-15].Cloud computing used service deployment technology that are provided by virtualization. The main advantages of the virtualization was that distributing the resources among multiple levels of service[16, 17] with the help of object virtualization that are network, storage, data, physical machine and servers[18].If the levels of service are explained only then the virtual machine are capable of delivering the services of the system to the end users. Virtual machine also capable for describing the information in a proper way and represent the resources in a set of entities that are logic-related for the end-users [19-21]. Virtual machine provide some application that are isolated in nature to the end-users with the functionality of the virtualized system and that application are running on the operating system. By using the Virtual machine the cost of resources are reduced for the end-users, saved the usage of energy and provide the easiest path for the maintenances of system[22-24].The main function of Virtual machine are independent in nature and provided the isolated platform to the users system component and protect the information of users from the attackers[25, 26].Attackers provided the controls of the Virtual machine in the context of the networking by attacking the provisioning and configuration module that are used for the formation of lowest layer that are reside on the hypervisor in cloud[27].The nature of the Virtual machine are dynamic so that it provide the level of difficulty to control the security of the system. Due to the nature of Virtual machine, the vulnerability of the system are also increased [28].By reducing the overhead of virtualization and reliability of system, Lin et al [29] proposed a technique that are used and supported the features of the hardware so that the performance of the Virtual machine easily improved that are known as hybrid virtualization. MDS technology are used for storing the data in different storage servers for protecting the loss of data from any kinds of disaster. MDS is a technique that are used for increasing the infrastructure efficiency and data reliability by using the different and distributed application and storage servers. For setup the connection of the distributed multiple services, the interconnection among the heterogeneous network are used in MCC[30].Some storage devices are available as infrastructure that are the major security concern for the users in MCC.MDS are used as a wireless technique among multiple location that are responsible for the infrastructure's changes. But this technique provided many problems such as disconnecting the servers, supplied incorrect signals and network management chaos. For reducing these problems, MDS provide technique to the end-user such as cloud base services [30].PPM is a technique that are commonly known as cloud based solution

and solved the problem of synchronous tasks by accepting the parallel data processing. This technique are used for drilling the tasks into multiple number of small tasks so that the tasks can easily solved in minimal time. For solving the problem of large sized information, parallel programming model was the best approach [31]. In the above description of the techniques are considered as a fundamental unit of cloud that are designed for the solution and the security concern. Now there are various section have the knowledge about the heterogeneous network that are used for providing the platforms of networking to the cloud computing.

B. HETEROGENEOUS FIFTH GENERATION NETWORKS

A heterogeneous network is considered as a wireless network that are used for the connection of portal devices with different operating systems and describe the explanation of the integrated network to the end-users. Heterogeneous network provide some protocols without any problem of manufactures. Heterogeneous network are also called mixture-style network that are used in the recently wireless area which support the advanced mobile broadcast services[49].In mobile broadcast services, new style of spectrums are used for increasing the compatibility and provided the fashionable improvement to the network performance. These spectrums required long time for providing the goal of the current methods [32]. Now focus on the previous information of the heterogeneous data in network, some features can be predicted for the future data of heterogeneous 5G of network in the context of mobile. The first one was introduced the explanation of the heterogeneous 5G that are used for improving the performance of the future devices. Mobile cloud have heterogeneous network that provided solution for improving the performance of network management and saved the energy usage trade-off [33].For improving the network management broadly, a technique are used such as leveraging distributed. These technique have the capacity to increase the 5G dramatically. Heterogeneous network are also used for the end-users so that they can easily switch network between the latest one 5G, 4G and the WIFI that are concern the security and the interoperability[34].There are many problem for adopting the MCC that is interferences and standardization among the networks and provide the intrusion properties with the attackers. There are some current intrusion detection technique that are used for the context of advanced wireless network.

3. INTRUSION DETECTION SYSTEMS

Intrusion may be defined as the set of attempts to compromise computer network security. Besides the several security services, Intrusion Detection System/Techniques are taken into point that strengthen the system security and is more powerful in preventing internal and external attacks. Intrusion can also be defined as an attack which can occur in any situation. Some tasks handled by IDS are

a. It prevents and mitigates the damage caused by intrusion.
b. It identifies the activity that can cause a more serious attack.
c. It identifies the attack perpetrator.
d. It discovers new attack patterns.

Some requirements that the IDS follow to fulfill its tasks include completeness, accuracy, performance, timeliness and fault tolerance.

IDS is classified into 5 categories:

a. Detection based on Anomaly (ABD)
b. Detection based on Signatures (SBD)
c. Hybrid Intrusion Detection
d. Stateful Protocol Analysis Detection (SPAD)
e. Detection based on Specifications (SPBD)

A. DETECTION METHODOLOGIES

This part includes the description of techniques, concepts, limitations and deployments of various IDSs including ABD, SBD, hybrid intrusion detection, SPAD and SPBD approaches.

1. SIGNATURE BASED DETECTION AND APPROACH

This technique is also known as Misuse Detection. It depends on the known patterns of unauthorized behavior [35]. It comprises of storing the signature profiles that identifies patterns that are associated with network intrusions in signature database and generates some rules that are based on signature profiles. The data packets that are transmitted on the network with their corresponding classification rules are classified on the basis of these generated rules. The intrusion patterns or strings on the database that are pre-installed, SDB depends on that. If SDB system is not updated, the signatures will not be detected that results in decrease of its performance. Since the intrusions are dynamic, the IDS using SBD may not identify new threats when connected to internet.

This problem can be solved by deploying an automated signature creator that is attached to this system [36, 37]. By collecting and analyzing the constituents of consistent behaviors, these signature creators can be generated [38, 39]. But this solution has also a limitation that the latest algorithms cannot completely detect all malicious instances. Due to the excess load of packets on network, the performance is deducted when the processing capability cannot match the

wireless transmission ability [40]. This can be solved if the data storage and processing can be moved to cloud and by examining the parallel signature matching on cloud based servers [41].

2. HYBRID INTRUSION DETECTION

Different types of intrusion depend on the security that are requested by the users [42, 43, 44, 45]. This type of intrusion detection are the combination of the two techniques that are called packet header anomaly detection(PHAD) and second technique called network traffic anomaly detection (NETAD)[46]. The limitations of these two technique are prevented by using the two components of detection such as misuse and anomaly. These two major components are designed by using the random forest algorithm [47]. These two techniques are designed on the bases of IDS which are used for the open sources assignment[48].The main aim of hybrid intrusion technique to increase the accuracy of the detection and decreasing the complexity of the network system[49].The hybrid intrusion detection technique are also used for enhancing the performance of the wireless network and designed the hierarchical structure of network[50].The main drawback of the hybrid intrusion detection was that in these it is difficult to combine the different types of detection techniques. In these multiple techniques are come to perform the tasks at the same time that's why the workload of the packets are increase.

3. ANOMALY-BASED DETECTION AND APPROACH

This system is an intrusion detection system which helps in detecting both network as well as computer intrusions and misapply by monitoring system activity and categorizing it normal or anomalous. The categorization is based on rules instead of signatures or patterns, and trying to identify any kind misapply that comes from normal system operation. The ABD system represents an approach of recognizing obvious separation or unpredictability in the events and transmissions [51, 52-54]. The collation if there is any separation in the usual and unfamiliar deportment and this unfamiliar deportment is observed to be dynamic or possible assault, which rely on the amount distinctness. There are three major techniques sustaining collations which contain mathematical-based [55], fact-based, and machine knowledge-based techniques [56, 57].

Mathematical-based (also referred as statistical-based) technique: This technique route each and every traffics and creates a description which analyzes if there might any kind of inappropriate traffic by a mathematical examination [58]. The problems for implementing mathematical-based technique are bifold. First, placing an actual stability between good or bad deportment is difficult. Second, if the system is being assaulted this technique may get failed.

Fact-based technique: It is a kind of computer program that make use of knowledge base to resolve complicated problems. This technique is relevant to those systems that have distinct knowledge structures or connected to set of rules [58], like symbolic representation.

Machine learning-based technique: Machine learning is a branch of computer science that provides computers the potential to know without being precisely programmed. In machine knowledge-based technique, [57, 58] latest deportment models which are based on the considerations of events, events, and activities are built.

4. SPECIFICATION-BASED DETECTION AND APPROACH

When compared with Anomaly-based detection, SPBD has almost identical mode for perceiving divergence but wants users to set up a behavior consideration level in a particular-requirement formation [60]. The stimulation for practicing SPBD system is to achieve excessive level of abilities in recognizing recent attacks and improving perfection. The SPDB approach is observed as a suitable result to inspecting the variable-extent patterns [61]. Although, identical to other ABD systems, the SPBD system too needs a large number of tasks for determining normal behavioral specifications.

5. STATEFUL PROTOCOL ANALYSIS AND APPROACH

The idea of stateful protocol analysis is basic to put stateful properties together to regular protocol analysis. The SPAD access of incursion investigation that differentiate inconsistent conclusions from regular courses in a period purchasing a preset global profile [62]. The profile supply ultimate users with an account of protected and reliable activity definitions. While performing the SPAD both the Datagram Protocol (UDP) as well as Transmission Control Protocol (TCP) will be assessed. [63]. This respective technique has the major absolute property which is supplying evaluation with stateful properties. In spite that the SPAD proposes powerful protocol analyses, there are two restrictions in practice. Furthermore, the difficulties of detecting assaults based on a particular request or retaliation are not fully fixed by that technique. Inscribing these difficulties, additional stateful properties required to be sum up with t the protocol analysis profile, which coincidentally claims large tasks and massive packets.

USER AUTHENTICATION

For the security, the high level of password are generated for the authentication's user. If the password of the user does not match then the user cannot get their information due to the security purpose. The main aim of the authentication was to ensure that the identities of the user was matched with the help of mechanisms of the authentication and randomly checked

that the user request are forward to the parties with the appropriate password [64].The mechanisms for testing the identities of the user is called biometric. The biometric mechanisms of the authentication checked the identities such as password (eye detection, finger prints etc.), behavior of the given characteristics [65-67]. This mechanism are used for the protection of the access user and supported by the password verification technique. This technique forward the data and the user information to the access user that are authentication for the data and create the privacy of data during the communication of the wireless network.

4. CONCLUSION AND FUTURE WORK

This technology of the networking are designed for the benefits of the user with the help of MCC and 5G heterogeneous network. IDS technique are used for the protection of the wireless networking communication with the help of protection the transmission of user data. This review paper discuss about the techniques of wireless network that are used for the communication and gave the outcomes based on the some achievements such as MCC, IDS and the 5G heterogeneous network. For securing the high level communication of the wireless 5G, introduced the framework that are based on the cloud intrusion detection techniques.

Based on these review paper, there are some questions that are introduced for the future work.

(1) How to solve the problem of security with the help of Cloud based IDS?

(2) If we generate some model such as energy aware model, how to fulfill the usage of the 5G heterogeneous network for the mobile cloud computing?

(3) How we can explain the transmission of secure data between the cloud based IDS and the users?

REFERENCES

[1] Huang, D. (2011). Mobile cloud computing. IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter.

[2] Intrusion detection techniques for mobile cloud computing in heterogeneous 5G Keke Gai1, Meikang Qiu1 *, Lixin Tao1 and Yongxin Zhu2.

[3] Kumar K, Lu Y. Cloud computing for mobile users: can offloading computation save energy? Computer 2010.

[4] Shiraz M, Gani A, Khokhar RH, Buyya R. A review on distributed application processing frameworks in smart mobile devices for mobile cloud computing.

[5] Miettinen AP, Nurminen JK. Energy efficiency of mobile clients in cloud computing, Proceedings of the 2nd USENIX Workshop on Hot Topics in Cloud Computing, Boston, MA, 2010.

[6] Simoens P, Turck FD, Dhoedt B, Demeester P. Remote display solutions for mobile cloud computing. IEEE Internet Computing 2011.

[7] Qiu M, Su H, Chen M, Ming Z, Yang LT. Balance of security strength and energy for a PMU monitoring system in smart grid. IEEE Communications Magazine 2012.

[8] Qiu M, Gao W, Chen M, Niu J, Zhang L. Energy efficient security algorithm for power grid wide area monitoring system. IEEE Transactions on Smart Grid 2011.

[9] Qiu M, Zhang L, Ming Z, Chen Z, Qin X, Yang LT. Security-aware optimization for ubiquitous computing systems with SEAT graph approach. Journal of Computer and System Sciences 2013.

[10] Hu F, Qiu M, Li J, Grant T, Taylor D, McCaleb S, et al. A review on cloud computing: design challenges in architecture and security. Journal of Computing and Information Technology 2011.

[11] Gai K, Li S. Towards cloud computing: a literature review on cloud computing and its development trends, 2012 Fourth International Conference on Multimedia Information Networking and Security, Nanjing, China, 2012; 142–146. IEEE.

[12] Marozzo F, Talia D, Trunfio P. P2P-MapReduce: parallel data processing in dynamic cloud environments. Journal of Computer and System Sciences 2012.

[13] Masdari M, Zebardast B, Lotfi Y. Towards virtualization in cloud computing. International Journal of Advanced Research in Computer Science 2013.

[14] Wang Y, Sun W, Zhou S, Pei X, Li X. Key technologies of distributed storage for cloud computing. Journal of Software 2012.

[15] Zhang S, Yan H, Chen X. Research on key technologies of cloud computing. In Physics Procedia. Elsevier: Beijing, China, 2012.

[16] Messaoud E HB, Diouri O. Web service security: overview, analysis and challenges. International Journal of Computer Science Issues 2014.

[17] Ma Z, Sheng Z, Gu L. DVM: a big virtual machine for cloud computing. IEEE Transactions on Computers 2013.

[18] Zhang S, Yan H, Chen X. Research on key technologies of cloud computing. In Physics Procedia. Elsevier: Beijing, China, 2012.

[19] Ma Z, Sheng Z, Gu L. DVM: a big virtual machine for cloud computing. IEEE Transactions on Computers 2013.

[20] Luo Y. Network I/O virtualization for cloud computing. IT Professional Magazine 2010.

[21] Chaudhary D, Chhillar RS. Reverse host allocation approach for virtual machine cloud computing environment. International Journal of Computer Applications 2013.

[22] Langer SG, French T. Virtual machine performance benchmarking. Journal of Digital Imaging 2011.

[23] Bright PP, Bijolin EE. Energy efficient virtual machine monitoring architecture for green cloud computing. International Journal of Computer Applications 2013.

[24] Lovsz G, Niedermeier F, Meer HD. Performance tradeoffs of energy-aware virtual machine consolidation. Cluster Computing 2013.

[25] Zhang F, Chen H. Security-preserving live migration of virtual machine in the cloud. Journal of Network and Systems Management 2013.

[26] Wang Z, Liu M, Zhang S, Qiu M. Sensor virtualization for underwater event detection. Journal of Systems Architecture 2014.

[27] Modi C, Patel D, Borisaniya B, Patel H. A survey of instrusion detection techniques in cloud. Journal of Network and Computer Applications 2013.

[28] Liao H, Lin CR, Lin Y, Tung K. Intrusion detection system: a comprehensive review. Journal of Network and Computer Applications 2013.

[29] Lin Q, Qi Z, Wu J, Dong Y, Guan H. Optimizing virtual machines using hybrid virtualization. Journal of Systems and Software 2012.