

Research on Security Architecture in Mobile Cloud Computing to Prevent Adaptive Anomaly Attacks

SMP Qubeb, Ilango Paramasivam

Abstract—Cloud Computing is a very viable data storage structure where the users can store and access the data from anywhere. Cloud computing use is increasing at a very rapid pace nowadays. But as cloud allows us data accessibility quite easily data security is a major concern and is an emerging area of study. Other issues related to cloud computing are data privacy and internet dependency. On the other cloud computing also has wide range of benefits over traditional storage and accessibility environment such as scalability, flexibility and resource utilization. We have worked in the area of mobile cloud computing to analyse and solve the problems of anomaly attacks. Our work focuses on preventing the adaptive anomaly attacks and some other security issues of cloud computing.

Index Terms— Joint probabilities, Machine translation, n-grams, Word Sense Disambiguation

1. INTRODUCTION

Cloud computing is basically outsourcing computer services. Users can simply use storage and computing services without having to worry about how it works internally. Cloud based technologies in these days have a lot of applications and is one of the most widely used technologies in the modern day world. Various aspects of the system such as security issues, environment friendly issues, mobile cloud storage are of significant importance here. We the common people would be evaluating based on the services provided to us. Common users do not see what the system behind the scene is. Thus the services rendered to us by the service providers should be fast, eco-friendly and most importantly of the least cost for the common man to use it. Of the vast applications of cloud computing some of the major ones include:-

- Cloud computing provides reliable and secure data storage center.
- Cloud computing can allow data sharing between different systems and via various networks at utmost ease.
- Cloud computing does not need high quality equipment for the user and it is user friendly.

The various advantages of cloud computing are cost savings, reliability and better manageability of humongous amount of data. Also, the various drawbacks are security, vendor-lock in, limited control over data access.

1.1 Cloud services Terminologies:

The various different terminologies used in cloud computing are:

1) Software As a Service(SaaS)

Cloud consumers release their applications in a hosting environment, which can be accessed through networks from various client. The end users of the cloud computing system do not have any control over the infrastructure of the System and thus the environment in which their data are stored is called SaaS. Motive behind implementing SaaS is to achieve economic optimization in terms of speed, security etc.

2) Platform as a service(PaaS)

PaaS is a developmental platform supporting full Software Lifecycle of the cloud computing infrastructure to develop cloud services.PaaS offers a development platform that hosts both completed and in-progress cloud applications.

3) Infrastructure as a Service

Consumers directly use IT infrastructures provided in the IaaS cloud. The basic implementation of the IaaS is to set up Virtual Machines(VM) that are isolated from the user which acts as an interface to the user to integrate and work with the different user functions and jobs.

4) Data as a Service(DaaS)

The delivery of data on demand is data storage service which is known as DaaS. This service is actually involved in the data storage of the redundant data over the cloud. Based on credential it would store and retrieve data for a user explicitly.

These terminologies are the basics of cloud computing and provide the criteria to judge whether any cloud system is up to the mark or not.

1.2 CHALLENGES OR ANOMALIES

- ✓ Security and privacy [13]
- ✓ Heterogeneity
- ✓ Performance
- ✓ Reliability
- ✓ Monitoring
- ✓ Standardization

2. ARCHITECTURE FOR MOBILE CLOUD COMPUTING FOR ANOMALY DETECTION

Revised Manuscript Received on April 12, 2019.

S MP Qubeb, School of CSE, Research Scholar@ Bharatiyar University, Coimbatore, T.N, India (qubebjntu@gmail.com)

Dr. Ilango Paramasivam, Professor, Dept. Of CSE, PSG Institute of Technology and Applied Research, Coimbatore-641062.T.N, India. (dr.p.ilango@gmail.com)

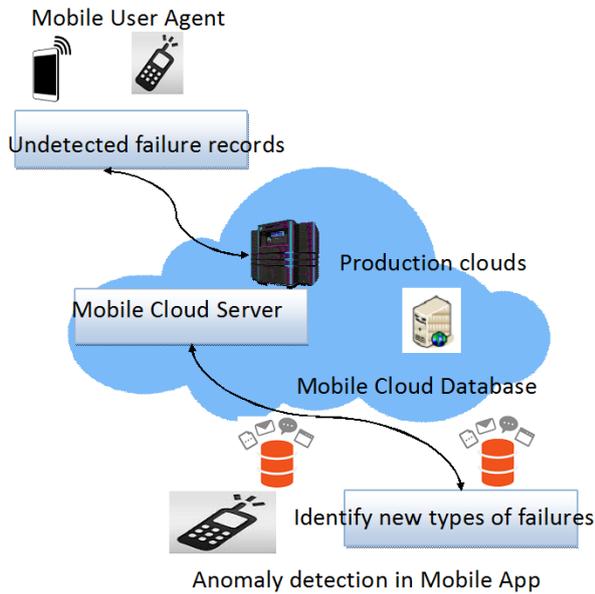


Fig.1 NOVEL SECURITY ARCHITECTURE FOR MOBILE CLOUD COMPUTING

Figure 1, represents the novel security architecture for mobile cloud computing. In general, mobile cloud computing have some mechanism for the working infrastructure. They are;

- ✓ Mobile User Agent
- ✓ Undetected failure records
- ✓ Production clouds
- ✓ Mobile cloud server
- ✓ Mobile cloud databases
- ✓ Anomaly detection in Mobile

In the proposed novel security architecture for mobile cloud computing, the cloud services layers are unable to detect the new types of failures in the mobile platform. In order to detect all the failures, the proposed Mobile Cloud Anomaly Detection (MCAD) algorithm has been proven effective. Initially, the Mobile user Agent will be login into the production clouds by giving the proper authentication details and start using the mobile data by various mobile cloud databases. Every data in Mobile cloud is not fully secured. So, in the mobile cloud computing, there are few security flaws that create the new types of failures. In order to prevent these Anomaly attacks, a proper methodology and algorithm is very much required in the cloud servers and production clouds. Our proposed work aims in delivering better prevention in anomaly attacks.

3. LITERATURE REVIEW:

In the research work of cloud based security attacks, the Portable frameworks [1] organization is one of the vital advances which support certain preparing. Overall there are two specific techniques in enabling remote compact units to talk with each other:

- 1) Infrastructure: Wireless adaptable frameworks have been by and large considering the phone thought and relied on upon extraordinary base support, in which the PDAs talk with get to centers like base stations which are connected with the changed framework system.

- 2) Infrastructure less: To the infrastructure less approach, the remote convenient framework is commonly known as the flexible uncommonly delegated framework Mobile Adhoc Network (MANET). This is a basic part of the correspondence advancement that sponsorships unavoidable figuring.

A flexible exceptionally named framework is gathering of remote center points that can be dynamically be set up wherever and at whatever point with no usage of past framework establishment. With augmentation of smaller devices and what's more progress in remote correspondence, exceptionally selected frameworks organization is grabbing its newsworthiness with the extending number of limitless applications. To choose the reasonable guiding ways and passed on messages in a decentralized space where the framework topology changes in far not precisely an especially described issue. New models are vital to depict the flexible improvised segment of the target remote frameworks, while new figuring are required for safely and successfully course information to compact objective remembering the true objective to support unmistakable applications intelligent media. The outstanding characters of MANET are to join development remarkable open entryways outrageous troubles.

Now personal computers (PC) are prepared for joining to the Internet from various spots inclined to create in notoriety until they govern people of the Internet. The issue of Mobile Networking [2] and Applications presents few research papers testing the effects of versatility on the Internet. As extended exchange speed ends up being more available and more information resources get the chance to be open by the technique for the Internet, the push for thought of remote capacities in the advanced mobile phones get the opportunity to be tenacious. If legitimate remote sign posts are incorporated for the auto transportation base, remote web enrolling could help in comprehension the profound pull ache for the customized managing on long auto trips. The physical layer, the objective is to recognize the signs between the two endpoints of a correspondence interface. The new remote media is getting the chance to be open among the vital drivers for the excitement for compact handling. A great deal of thought must be paid to strategies for setting up associations between versatile PCs and base stations for get to centers. Phones are using diverse headways [10] can give incredible breadth inside the United States, parts of Asia, and Europe, regardless of the way that there is no single development so far giving sufficient broadness of degree. Weight is much of the time charming in light of the way that it diminishes the information transmission necessities, and that can be basic for low-speed remote media.

In [3], an adaptable versatile framework is modestly new term for an old advancement - a framework that does not rely on upon existing establishment. The centers in a MANET can be effectively join and leave the framework, from time to time, consistently without notice us, and maybe without making intrusion other center points'



correspondence. Instances of use of the MANET are key operation, shield missions, national security, law necessity, business use, guideline, sensor frameworks. Center points in MANET show nomad lead in uninhibitedly moving inside some region, dynamically by making and tearing down association with various centers. Social occasions of the center points [9] that have a common target can make the game plans (groups) and move together. MANETs can be perceived from other extraordinarily named frameworks by the rapidly changing framework topologies, influenced from the framework size and center point mobility. The crucial troubles in the arrangement and operation are of the MANETs, stood out from the more standard remote frameworks and the way that all correspondence is preceded with remote medium. In Multiple Access Collision Avoidance (MACA), proposes the usage of RTS/CTS talk for the effect evading on the shared channel. The essential favored stance of the given single-degree coordinating traditions, is in relationship with the multi-scope controlling traditions, and their lower unusualness.

In [4], Portable Ad-hoc Networks (MANET) is creating area of research in most of the countries. Most present work is focused just on coordinating issues. Adaptable Ad-hoc Networks (MANET) is raising domain of research in most of the countries. Most present work is focused just on coordinating issues. As both the clients and servers are adaptable, the speed with which the framework topology changes can be snappy. Center points may not stay connected with framework for the term of their life. To be connected with the framework, the center point must be inside the district of effect of no short of what one other center of the framework. Data correspondence in convenient databases is limited in light of conditions were simply the clients are adaptable and battery filled. A MANET may consolidate the data pull, data push and circulated correspondence. The data correspondence issues in MANET databases are engaged to two territories. The main area concerns the hindrances of environment (remote, limited information exchange limit, battery filled). The other region concerns various courses in which data correspondence may happen. Of all the MANET works out, data correspondence remains as one of the capable usage works out. With data respectability, we are stress with the precision of information set away at each center point: server and client. Future research ought to begin in tending to these issues. Close by these issues, organized benchmarks and the criteria for evaluation must be set up.

In [5], In the last late decades, the flexible using has been developing everywhere, and practically 25 billion devices are depended upon to be interconnected as a result of the

continually open system. The 1G advancement contains straightforward based systems, which displayed reliable compact system that presents flexible voice organizations. 2G is a propelled remote structure which uses different access through Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA), making it more efficient to the extent data organizations, flexibility organization and range efficiency. The 3G continued with its progression in the way towards a prevalent system, transporter accumulation, higher data rates, and updated flexible broadband experiences. 4G gives compact frameworks ability to pass on progressively constrain for speedier and better adaptable broadband experiences, and unendingly keeps creating to give more data farthest point, and furthermore snappy and with continuous affiliations. On account of the colleague of new radio access with headways and the development towards the IP-based outline, new vulnerabilities have been brought into the framework designing. Dealt mobile phones can be in like manner be used to dispatch attacks on convenient frameworks. Other spreading systems is used to exchange off a mobile phone consolidate permitting of the assents from dangerous applications. Guaranteeing and securing adaptable frameworks is still an imperative concern. In light of the improvement in the convenient framework outline, a couple of inadequacies have been acquired to the framework. Introducing new threats, this can be used to perform attacks in E-UTRAN and the EPC. These ambushes can even target both the AS and NAS traditions inside the C-plane and the U-plane.

The research in [6] is divided into two phases; first one being the analyzing the pattern of the security attacks and issues taking into consideration the mobile devices and gateway. It also gives an authenticated way of encryption and securing the data. The second phase basically focuses on the infrastructure and using simulation models to combat issues regarding the security.

The paper [7] mainly focuses on the various optimization ways of mobile cloud computing and the various drawbacks which is faced by the various mobile devices and also the quality of the communication. It also provides a solution to combat the security related issues which give high end result.

The paper [8] discusses about the various types of models used for deployment in computing based on cloud. It also focuses on the various cloud based models and the architectures and their corresponding features. It also gives the open issues that prevail in the sector of mobile cloud based computing.

Table.1 *COMPARISON OF VARIOUS SECURITY ISSUES IN MOBILE CLOUD COMPUTING*

Approach	Cloud level trust	Security attribute provided	Third party security	Advantages	Disadvantages
RSA algorithm	Trusted	It involves the keys, their generation, encryption and the key decryption.	Yes	It describes design which is required to secure the privacy of the user of the mobile system.	It does not give an insight into the various architectures of the mobile cloud.
Management of digital rights	Trusted	Providing of keys, namely, for encryption and decryption.	Yes	It discusses in detail all the various methods that are required to secure a mobile cloud.	No disadvantages.
Encryption	Trusted	Translation of data into a secret code.	Yes	It focusses on encryption for the prevention of the system from getting hacked.	It does not provides the core solutions to the problem or the issues.
Trust based	Not trusted	none	No	It explains various security issues and these effect the data and the related apps.	It does not gives core solutions for the issues.
Backend structure of the mobile system.	Not trusted	To know how the mobile device will be connected to the cloud.	No	It gives detailed information about the various types of application in mobile systems and other types of services provided by the cloud.	It does not gives an insight about how the security issues can be resolved.
Simuation models	Trusted		Yes	It gives useful solutions to combat the security issues regarding the mobile cloud.	No disadvantages.
Elastic division	Not trusted		No	It gives optimized solutions to security issues and privacy related problems.	No disadvantages
Message authentication files and encryption.	Trusted		Yes	It gives suitable solution to all the security issues.	No disadvantages
Data security plan	Not trusted		No	It gives a framework to combat the security related risks.	No disadvantages
None	Not trusted	none	No	It drastically reduced cost of communication by using data present in cloud(historical data)	It take more processing time and energy of mobile device

4. PROPOSED ALGORITHM FOR ADAPTIVE ANOMALY DETECTION IN MOBILE CLOUD COMPUTING

By analyzing number of security flaws and issues, the mobile cloud computing require better security from the various other devices. Our proposed algorithm for Adaptive Anomaly detection in mobile cloud computing have been sensibly analyzed and given as an algorithmic observation for implementing it on any production clouds or cloud server.

4.1 Algorithm for Anomaly detection in MOBILE cloud computing

Acronyms

- **PCS** - Production cloud server
- **MCAD** - Mobile Cloud Anomaly Detection server
- **M-UID** -Mobile User Identity



Our proposed Algorithm for Adaptive Anomaly detection in mobile cloud computing involves three Steps:

- ✓ Generating the M-UID in PCS
- ✓ Encrypting the Mobile data in PCS
- ✓ Decrypting the Mobile data in MCAD server

1. Generating the initial M-UID

Before the user data gets encrypted, mobile user ID generation have been done by the production Cloud server

2. Let R be a pseudorandom function, let k_p be a pseudorandom permutation and let HC be a cryptographic hash function.

Generate $k_p(r) = (HC(R), g)$ and $k_p(UID) = (PCS, HC(R))$, such that

$HC(R) = 1 \pmod{k_p, R}$, R has been a large secure prime such that $R > \lambda$ and $PCS > \lambda$, $k_p(r)$ is a generator of M-UID

Output in M-UID $HC(k_p(r))$ results in detecting different anomaly (failures) in MCAD server.

5. RESULTS AND PERFORMANCE EVALUATION

5.1 Simulation setup and metrics

In Mobile Cloud computing, the response time analysis is one of the important feature for calculating the performance of the system with respect to the mobile cloud. We have implemented this particular model in java programming and included the package in the dynamic cloudsim tool for getting our results. There are some general assumptions we need to make in order to think about the real time scenario. Hence, assume there are three production cloud servers deployed in an industry. Now in our testing methods in dynamic cloudsim, the user mobile identities have attacked by some cloud server attacks such as flooding of request of individual mobile nodes are presumed to have more threats. Here in our analysis, we have carefully taken consideration of a regular model table and a pictorial graph for the better understanding. From the table 2 results, the encryption in the mobile cloud and response time reduction from our proposed algorithm has been shown clearly in the figures 2.

During Adaptive Anomaly detection in mobile cloud computing that always needs the throughput decreases due to the overflowing congestion in the mobile clouds. The simulation results and graphs in figure 4 represents after applying our proposed algorithm the throughput increases. Also, our proposed model has been compared with MIDS (Mobile Intrusion Detection system) model, and the results shown are comparatively better than the existing methods.

Table 2. Throughput Analysis

No. of Packets	Throughput (mbps) during attack - Proposed model	Throughput (mbps) during attack - MIDS model
100	44	30
200	65	42
300	110	86
400	136	92
500	150	101

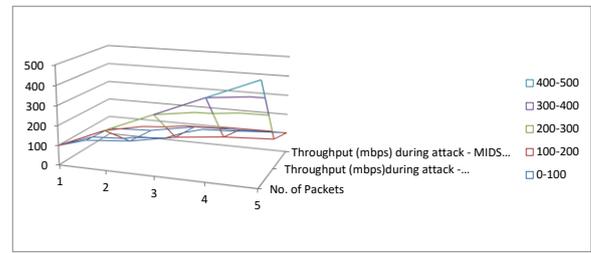


Fig.2 Throughput in mbps Analysis comparison in Adaptive Anomaly detection in mobile cloud computing

6. CONCLUSION:

The main topic of our study is mobile cloud computing. Cloud computing is a modern technology developed where users can use the system to upload huge amount of data and retrieve it later anytime anywhere. The system has been developed recently so it has some loop holes as of now and the major one out of them is data security. Although we, the end users find it very attractive in our day to day lives while using cloud storage we have to pioneer to the fact that companies need to develop their security of cloud storage more. There has been huge amount of research going on data security in cloud and still researchers are coming up with new ideas. But the major part is their implementation. Moreover the increasing securities risks that cloud computing are inheriting these days are a major concern. In Anomaly attacks, intermittent user intrusion is some of the factors which are up and about to destroy the cloud storage integrity these days. Thus the security privileges should be increased as data integrity is very important when it comes to data management of big companies where privacy of the data stored is very important. At last to conclude cloud storage is revolutionizing the way data is stored now a days and with the inclusion of companies like Google cloud storage is ready to reach new heights and if used the right way in the future would be replacing all kinds of physical data like hard disk, floppy drives, USB etc. which have higher rate of intrusion of privacy than cloud storage.

REFERENCES:

1. Mitra, R. N., &Agrawal, D. P. (2015). 5G mobile technology: A survey. ICT Express, 1(3), 132-137.
2. Chlamtac, I., Conti, M., & Liu, J. J. N. (2003). Mobile ad hoc networking: imperatives and challenges. Ad hoc networks, 1(1), 13-64.
3. Kahn, J. M., Katz, R. H., &Pister, K. S. (1999, August). Next century challenges: mobile networking for "Smart Dust". In Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking (pp. 271-278). ACM
4. Inoue, A., Saito, M., & Iwashita, M. (2015, July). Behavior Analysis on Mobile-Carrier Choice & Mobile-Phone Purchase. In Applied Computing and Information Technology/2nd International Conference on Computational Science and Intelligence (ACIT-CSD), 2015 3rd International Conference on (pp. 422-427). IEEE.



5. Patel, K. N. (2015). A survey on emulation testbeds for mobile ad-hoc networks. *Procedia Computer Science*, 45, 581-591.
6. Chaturvedi, Manmohan, Sapna Malik, Preeti Aggarwal, and Shilpa Bahl. "Privacy & Security of Mobile Cloud Computing." *Ansal University, Sector 55* (2011). Mandeep Kaur Saggi, Amandeep Singh Bhatia, A Review on Mobile Cloud Computing: Issues, Challenges and Solutions, June 2015.
7. Malik, S., & Chaturvedi, M. M. (2013). Privacy and Security in Mobile Cloud Computing. *International Journal of Computer Applications*, 80(11).
8. Sekaran, Kaushik, Mohammed S. Khan, Rizwan Patan, Amir H. Gandomi, Venkata Krishna Parimala, and Suresh Kallam. "Improving the Response Time of M-Learning and Cloud Computing Environments Using a Dominant Firefly Approach.", Volume: 7, Page(s): 30203 - 30212, DOI: 10.1109/ACCESS.2019.2896253, *IEEE Access* (2019).
9. Sekaran, Kaushik, and P. Venkata Krishna. "Big Cloud: a hybrid cloud model for secure data storage through cloud space." *International Journal of Advanced Intelligence Paradigms* 8, no. 2 (2016): 229-241.
10. Sekaran, Kaushik, and P. Venkata Krishna. "Cross region load balancing of tasks using region-based rerouting of loads in cloud computing environment." *International Journal of Advanced Intelligence Paradigms* 9, no. 5-6 (2017): 589-603.