IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 9, PP 33-39

Secure Storage For Ad Hoc Cloud

Vijay Singh[1], Nitin Yelwande[2], Swapnil Kokani[3], Dr. Mamta Meena[4]
[1,2,3](Department of Computer Engineering, Atharva College of Engineering, India)
[4](Assistant Professor, Department of Computer Engineering, Atharva College of Engineering, India)

Abstract: *The rapidly increasing growth of technology has seen the rise of technologies like cloud systems among others. The use of these cloud systems enables people to back up their data and access it whenever needed. However, an internet connection is required. There are some instances, for mobile clients, where a continuous network connection is not available and in such cases the cloud cannot be accessed. We may make use of an ad hoc cloud system but the major issue with these is the lack of security and lack of a centralized authority. In this paper, we will be analyzing the SAS Cloud: ad hoc cloud for secure storage. The SAS (Storage as service) cloud provides a centralized authority for data storage even in network disconnected areas and provides a high level of security. We will focus on simulating the various conditions and situations that may be encountered using a simulation software. The results can then be analyzed to see the feasibility of such systems and their overall utility.*

Keywords – *Ad hoc cloud, distributed storage, mobile cloud*

I. Introduction

Mobile cloud computing is steadily becoming an important term. Almost all data in this day and age is stored on servers based on devices that support cloud storage [4]. The data can be in any form like photos, videos, text, documents etc. There are different companies that provide cloud storage services like Google, Apple, Dropbox etc. But these services need continuous network connection and without network connection they are useless. The SAS (Storage as service) Cloud removes this con by using pre-built Wi-Fi and Bluetooth to share data to a neighbouring node of any device. SAS Cloud is an ad hoc cloud system that provides secure storage services in network disconnected areas [1] [5]. The mobile user has to register his mobile device to SAS Cloud central authority (CCA) and become a registered mobile (RM) node. When a client sends data to a RM node, it needs assurance that the data is secured, and it is transferred to cloud storage and whether the RM node should be trusted or not. For this each RM node gets performance point (PP) that specifies its trustworthiness within the framework. SAS Cloud has some registered cloudlets that are used for content collection and integration. Cloudlets search for interested RM nodes in the neighbourhood whenever a client needs to use the storage service. These RM nodes are in the range of the client and can be used to create an ad hoc cloud. Data confidentiality is ensured as an encryption system is used and the main idea is making sure the SAS cloud is available in the maximum number of regions [6]. It is easy to use which allows more users to participate and divide the data and distribute for fast and secure connection. All these client and RM nodes must be verified by CCA to download and upload the data.

II. Need

2.1 Motivation

In the 21st century internet connection is important as electronic data interchange is done a lot and people have limited storage. To solve this problem, we use SAS Cloud to share the data from the client device to the RM node to free the space and later get that data from CCA when needed. This provides free storage and data sent to RM node is secured and stored in Cloud Storage. With the day to day increase in population more people can use this system to distribute their data and free their storage. Many other companies give cloud services with lots of storage data for their users but they need continuous data connection to transfer the data. In SAS Cloud default connection is required like Bluetooth and Wi-Fi which all devices have.

2.2 Basic Concept

The SAS Cloud system provides functionalities such as reduced costs, ease of use and better accessibility. It also allows transferring data from client to cloud storage without continuous data connection/ no internet connection. SAS Cloud uses client and RM node to interact with each other to get data from client and send it to the RM node. RM node will move to nearest cloudlet and transfer the data of the client which is encrypted and send it to the cloud central authority (CCA) after verifying itself to it for authenticity. When the client will be in any of the cloudlet it will automatically download the data from the CCA that was given to RM node to store.

III. Related Work

An ad-hoc cloud is comprised of mobile nodes with no-exclusive and sporadic resources, where nodes do not have any pre-commitment to each other. Some of the different mobile computing platforms are Hadoop Apache, BOINC, clone cloud, considered energy efficient mobile devices to provide a feasible and energy efficient mobile cloud. Such systems require continuous Internet connection which is not possible in rural areas. Even in urban areas, we cannot expect the continuous presence of wireless points. But there are researchers who came up with the formation of opportunistic cloud system by considering the nearby device, its computing power and dividing and distributing the resource. This architecture does not require any Internet connection but there exists a high risk of security breach. In the absence of continuous control of any centralized authority, clients often lose control over the outsourced data and fail to detect the dishonest mobile devices and cannot protect the valuable information from attackers. S. Al Noor et al. [1] propose an ad hoc cloud system that provide secure storage service in network disconnected areas such as in rural areas. They propose the black box map-based content distribution algorithm for efficiently distributing clients content without revealing mobile device's future location information to other clients. They demonstrate the feasibility and performance of proposed SAS Cloud model via simulation and analysis of experimental results.

Delay tolerant Networking is increasing rapidly to enable communication in network challenged areas. Nodes communicate via asynchronous messages of arbitrary size that are exchanged using the store carry forward method. Ari Keränen et al. [2] created the Opportunistic Network Environment (ONE) simulator in order to accurately simulate the working of delay tolerant networks. ONE simulator is managing the node movement, inter-node contact, routing and message handling. Plenty of tools are made available by opportunistic networking evaluation. These tools allow us to create realistic and complicated node mobility environments. The ONE simulator has a very adaptable interface for input and output. The GPS map data allows for enhanced and varied node capabilities and activities.

Ad hoc cloud uses resources that are not exclusive, available irregularly and have no reliable infrastructure as such. There is no level of trust between the end user and infrastructure provider. It targets a set of more diverse applications such as memory, I/O and disk intensive task as opposed to typical CPU intensive applications commonly executed by volunteer computing systems. G. McGilvary et al. [3] came up with the solution to above given challenges by developing an ad hoc cloud computing solution. They provide an overview of the concepts and foundations of ad hoc computing and implementation. The ad hoc cloud concept is useful for those who wish to improve their infrastructure efficiency and utilization as well as reduce costs by improving their return on IT investment.

H. T. Dinh et al. [4] in their paper provide in extensive detail the terms and definitions related to mobile cloud computing and give us a clear idea of the entire concept and its various advantages, applications and architecture. Mobile cloud computing simply defined refers to the infrastructure that allows for both data storage and processing to happen outside the mobile device. This results in improved data processing and data storage capabilities, longer battery life, greater reliability and ease of integration. Due to its various advantages, mobile cloud computing finds it use in a wide variety of fields like mobile commerce, mobile learning, mobile healthcare and mobile gaming. It is also used whenever we need to search for specific information, video, images etc. Despite all these advantages there are still plenty of issues involved in mobile cloud computing. The limited bandwidth available has to be shared among all users and this leads to significant problems in terms of speed. There is also the fact that there are certain instances where there is no network availability. In such cases, the mobile cloud computing network cannot be accessed. There is also the issue of the security and privacy of users being compromised.

A mobile ad hoc network refers to a temporary network that can change locations and be configured without having to stay at one location. H. Alshareef and D. Grigoras [5] in their paper observe that managing MANETs is a difficult task and thus propose a new method of MANET management using cloud services. MANET management is quite complex and thus results in high resource consumption on mobile devices. One of the main issues is the allocation of IP addresses and subsequent monitoring to ensure that there are no duplicates. This occurs during processes like joining and splitting of networks or when a new device joins or exits the network. The proposed solution in the paper states that instead of carrying out MANET management on middleware systems on mobile devices, we should instead use a cloud for managing the MANET. This assumes that one of the mobile devices is connected to the internet and thus all mobile devices have access to the cloud.

M. Suguna et al. [6] in their paper cover the fact that mobile cloud computing while convenient in its ability to allow users to share third party resources for storage and computational tasks; opens them up to the risks associated with sending data wirelessly like phishing, skimming, identity theft, snooping, eavesdropping etc. Identity management refers to the process of managing, verifying and authenticating the identity of users in order to ensure that only the correct people have access to sensitive information. Here they propose a new Secure Identity Management System (SIDM) in order to overcome the vulnerabilities present in the

Consolidated Identity Management System (CIDM). These vulnerabilities are traffic interception and compromise of mobile device or server. The SIDM makes use of two step authentication process that involves token verification as well as Zero Knowledge Proof (ZKP). This method allows for much greater amounts of security at the cost of slightly increased communication overhead between the IDM and cloud service provider.

In today's world healthcare is a major issue for a large majority of people. Due to the advancement of technology, the quality of healthcare being provided has also improved. Companies have made gadgets for patients or people to track their health issues by using sensors on them. These sensors send data to the cloud for storage and for managing data. These gadgets are wireless and can be used anywhere in remote areas and also for people who may not have easy access to hospitals like the elderly and disabled. IoT can be used to store the data online. There are a number of gadgets that can track an individual's vital signs like pulse rate, blood pressure, body temperature and respiratory rate. C. Doukas and I. Maglogiannis [7] have proposed a system where they used cloud storage to store the medical data from the patient using wireless communication. These data can be of any form like temperature, location, ECG, oxygen saturation etc. It can be calculated by any devices that supports the system such as mobile phones or smart watches. It usually uses user-friendly GUI to interact with user and sends data to cloud storage. The system uses both software and hardware to gather the data from sensors and store in cloud storage.

N. Zingirian and C. Valenti [8] describe the Vehicle Communication Platform(VCPs), which is based on cloud computing concept. It uses the sensors on the vehicles to track the vehicles in real time and this is done by a third-party monitoring application. The main concept is to monitor trucks in Europe on a real time basis. Today all the details of vehicles are digitally generated due to increase in vehicles population. The Intelligent Truck Monitoring (ITM) is making a new system for communication between them to track them properly and use that data precisely for more accurate route choices. They are highly flexible and can also be used for tracing, tracking and vehicle localization. The VCP is comprised of on board units (OBUs) in vehicles as well as a service centre connected to OBUs by mobile networks. By using this system in cloud storage, they can track, trace and locate the vehicles easily due to VCP and ITM technology.

S. Chatterjee and S. Misra [9] proposed a system for tracking multiple agents/targets by sensors using sensors-cloud. As any target enters any coverage area where multiple sensors are present, the system will select or schedule a sensor to the target. It has to work hard as it can get complicated by overlapping coverage or to maintain their privacy. To avoid these issues, they have proposed a Dynamic Mapping Algorithm(S-DMA). Each target is approached as a single unit and uses wireless sensor Network(WSN) which sends the data to the cloud storage of that area. By using S-DMA it gives the best allocation to the sensors targets. Two sensors can be heterogeneous so to avoid this they used a protocol standardization.

Road accidents are among the leading causes of death and injuries worldwide. There are various factors that lead to road accidents and the need of the hour is to address this issue and make roads safer for all who use them. S. Sultan et al. [10] propose the use of vehicular ad hoc network (VANET). VANET simply explained is a short range ad hoc network created between vehicles on the road. Dedicated short range communication (DSRC) is used to communicate with other vehicles on the road as well as fixed equipment on the roadside. The idea is that by allowing vehicles to share information drivers can be aware if any accidents have occurred on their route ahead or about particular road conditions. It also informs the user if they are violating any rules of the road and provides assistance while making turns. Users are made aware of road signs they are passing by and any blind spots up ahead to ensure they are informed. These features ensure that drivers can get from one place to another safely. There are various challenges that come in the way of implementation of VANET. These include signal fading due to obstacles, bandwidth limitations, connectivity issues and security and privacy of users. Despite these hurdles it remains a great way to address the issue of road accidents.

IV. Previous System

SAS Cloud computing has become very popular over the last couple of years. Several market observers are of the mind that this is the technology that will shape our future. Despite these positive signals there are several security problems still present [6]. The use of mobile devices like smartphones and tablets along with the widespread use of the internet have lead to the accelerated growth of cloud computing. Lots of people carry their portable devices and easily access their documents, media and pictures on cloud storage via the Internet [4]. With the development in technology, users are also worried about the increased security needs for cloud computing. The "cloud" in cloud computing can be defined as the set of devices, networks, storage and services that combine to deliver aspects of computing as a service. The present system uses node-based approach, in which RM node receiving any content estimates the time to meet the nearest cloudlet on its way [1]. The SAS Cloud is a combination of three service models, such as network as a service, Infrastructure as a service and Platform as a service. It needs only two devices to do the job- client and RM node.

Fig. 1: Registration of RM Node

Data privacy is ensured using encryption algorithms to strengthen the security of the cloud. Client and RM node communications are secured using digital signatures. Data is transferred remotely as the cloud network is a virtual environment. Private key and public key is used in this security level in SAS Cloud and hash table is used.

In step 1, the RM-Node delivers the encrypted content, and signatures and certificates of the RM-Node and client to the cloudlet.

In step 2, the cloudlet verifies the signatures of the RM-Node and client. The cloudlet discards the content if any of the signatures does not match.

In step 3, the cloudlet stores the hash and the metadata of the content (C − Data), such as RM-Node's id, CE, signatures of the Client and the RM- Node.

In step 4 and 5, the cloudlet creates a signature, and sends the S-cloudlet to the RM-Node. The RM-Node stores the S-cloudlet as proof that the cloudlet has received the content.

In step 6, the client sends a request message to the cloudlet along with its certificate and hash value of the content.

In step 7, the cloudlet retrieves the C − Data using the provided hash and verifies Sc.

In steps 8 and 9 the content is delivered to the client by the cloudlet along with a signed acknowledgement (Sc-ack). The signature is stored as proof by the cloudlet that the content has been received by the cloudlet.

V. Proposed System

In this system we are using Cloudlet Meeting Time Prediction (CMTP). The Client predicts the RM -Nodes nearest to the Cloudlet and also the time it will require to meet. The Client checks the location and time of the RM -Node in regular time intervals to checks the position of the RM-Node on Map. The problem with this approach is that the client can track all the future location of an RM-Node. To hide the location and ensure the privacy we are using black box based approach. The RM node provides location information directly here and so to ensure privacy it sends the location information in an encrypted manner. RM node and CCA use a pre-shared key K for encryption purposes.

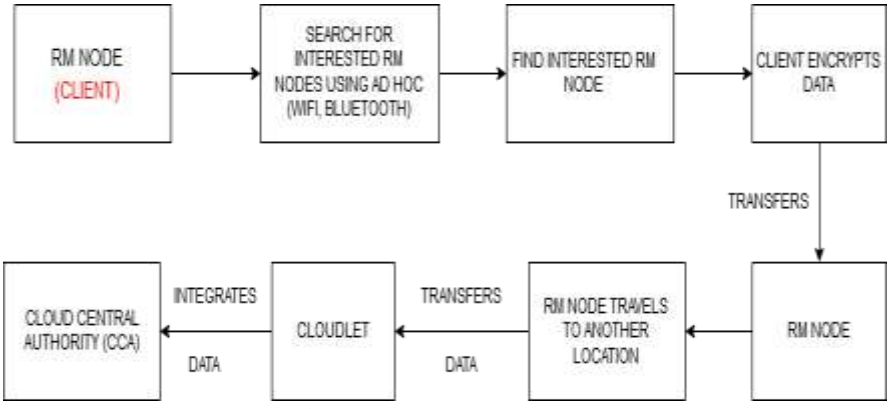

Fig 2: Data Transfer Process

Every RM node device has the black box program installed. In addition to containing the CMTP algorithm, it also provides a hash table that maps each RM-Node's id with the pre-shared key. The black box is designed in such a way that the client neither can see nor can manipulate anything inside the black box. In other words, the black box only takes encrypted location information as input and delivers time as output without revealing any key or location information.

Fig 3: Data Retrieval Process

We will be making use of Opportunistic Network Environment (ONE) simulator which is an open source, Java-based simulator in order to carry out simulations in various different circumstances with varying parameters. From running the simulations and analysing the results gathered we will determine the feasibility, advantages and shortcomings of such a system.

VI. Architecture

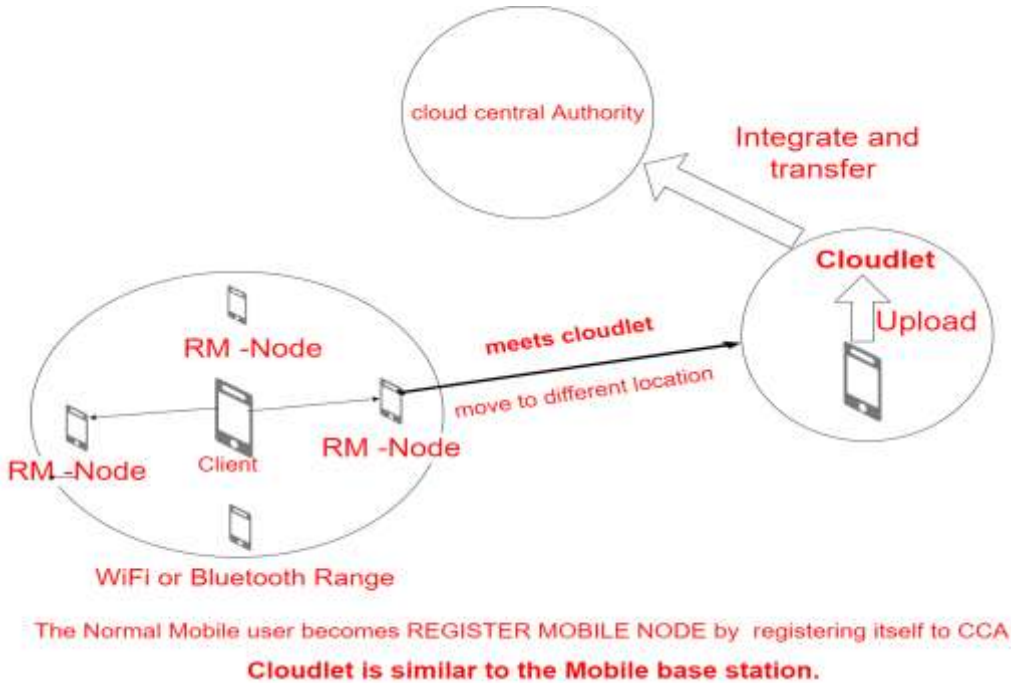

Fig 4: Ad hoc cloud architecture

6.1 Cloud Central Authority (CCA)

In order to participate in the ad hoc cloud, a mobile user first has to make sure that their mobile device is registered with the CCA. The CCA is basically the central authority that keeps track of all devices.

6.2 Registered Mobile (RM) Node

After any user has registered their device on the CCA, that device is referred to as RM node. Once the registration with the CCA has been completed, the user device is assigned a Performance Point (PP). The PP is a measure of how reliable a device is for a certain task based on its past performances. The PP is not stagnant and keeps on changing based on how well the device performed its previous task.

6.3 Cloudlet

A cloudlet can be compared to the cellular base station of mobile networks. The cloudlet allows communication between different RM nodes and has the necessary storage in order to store and forward any content that has been delivered to it for further communication.

VII. Expected Results

In this paper, we simulate a centralized ad-hoc cloud system that provides storage services. It is a delay tolerant network that allows for breaks in the transmission of data. The efficiency of the process can be determined using among other factors- the time taken to meet the nearest cloudlet. The time taken to meet the nearest cloudlet can be predicted using different algorithms namely the greedy based algorithm and the Cloudlet Meeting Time Prediction (CMTP) algorithm.

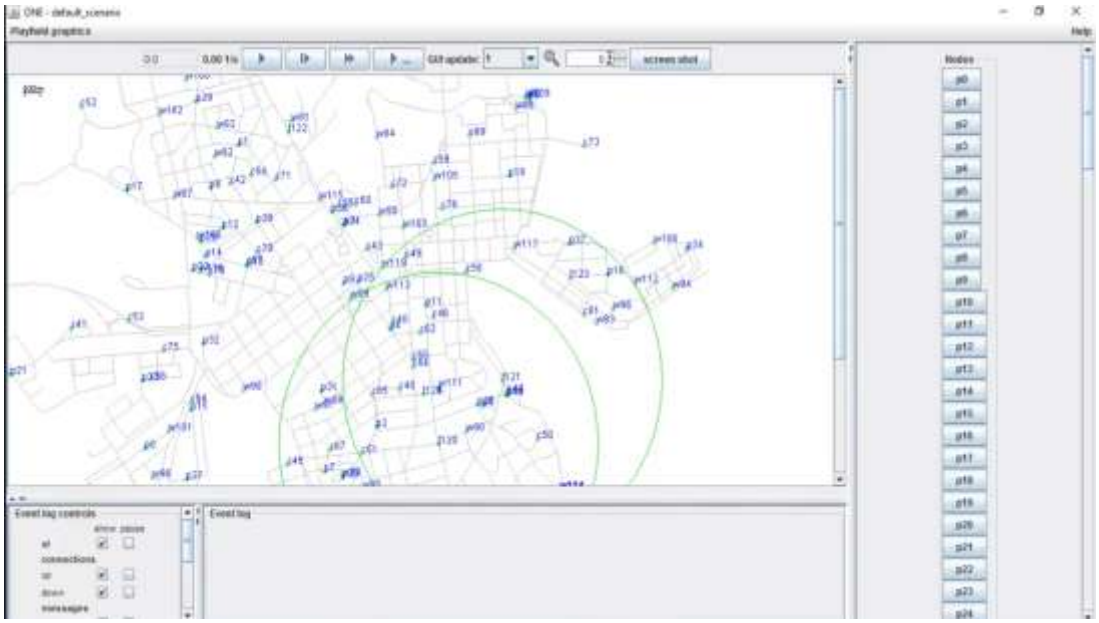

Fig 5: The ONE simulator GUI

After performing simulations on the ONE simulator we expect the results to show that the efficiency of the CMTP algorithm is much better than the greedy based algorithm. Therefore, it would be much faster with significantly reduced content delivery times.

VIII. Conclusion

Cloud storage services provide us the luxury of being able to upload data and access it whenever it is convenient for us. The need for continuous network connection is somewhat of a barrier during instances and situations where we are in network disconnected areas. In this paper we explored the idea of using SAS Cloud ad hoc cloud for the purpose of backing up data in areas without network connection. Ad hoc cloud services are the way forward in terms of increasing the reach and ability of present cloud systems. Though they pose difficulties in the form of security and lack of centralized authority, when these challenges are addressed we are left with a powerful system.

References

[1] S. Al Noor, M. M. Hossain, R. Hasan, "Sascloud: Ad hoc cloud as secure storage", *Proc. of the BDCloud*, 2016

[2] Ari Keränen, Jörg Ott, Teemu Kärkkäinen, The ONE simulator for DTN protocol evaluation, Proceedings of the 2nd International Conference on Simulation Tools and Techniques, March 02-06, 2009, Rome, Italy

[3] G. McGilvary, A. Barker, M. Atkinson, "Ad hoc cloud computing", *CoRR*,2015

[4] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Wireless Communications and Mobile Computing, vol. 13, no. 18, 2013

[5] H. Alshareef, D. Grigoras, "Mobile Ad-hoc Network Management in the Cloud", *Parallel and Distributed Computing (ISPDC) 2014 IEEE 13th International Symposium*, pp. 140-147, 2014

[6] M. Suguna, R. Anusia, S. Mercy Shalinie and S. Deepti, "Secure identity management in mobile cloud computing", 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2)

[7] C. Doukas and I. Maglogiannis, "Bringing iot and cloud computing towards pervasive healthcare," in IMIS, 2012

[8] N. Zingirian and C. Valenti, "Sensor clouds for intelligent truck monitoring," in IEEE Intelligent Vehicles Symposium (IV), 2012

[9] S. Chatterjee and S. Misra, "Target tracking using sensor-cloud: Sensor-target mapping in presence of overlapping coverage," IEEE Communications Letters, 2014

[10] S. Sultan, M. Doori, A. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," Journal of Network and Computer Applications, vol. 37, 2014