

A Novel Privacy and Security Framework for the Cloud Network Services

Irish Singh*, Kamta Nath Mishra*, Antonio M. Alberti**, Antonio Jara***, Dhananjay Singh****

*Dept. of Computer Science, Birla Institute of Technology (BIT), Mesra (Allahabad Campus), India

**ICT Lab, National Institute of Telecommunications (INATEL), Brazil

***Institute of Information Systems, University of Applied Sciences Western Switzerland (HES-SO) Sierre, Switzerland

****Dept. of Electronics Engineering, Hankuk University of Foreign Studies (HUFS), Yongin, South Korea

singhirish@gmail.com, knmishra@bitmesra.ac.in, alberti@inatel.br, jara@ieee.org, dan.usn@ieee.org

***Corresponding Author: dan.usn@ieee.org

Abstract— This paper presents an overview of security and its issues in cloud computing. Nowadays cloud computing has tremendous usage in so many fields such as financial management, communications and collaboration, office productivity suits, accounting applications, customer relationship management, online storage management, human resource and employment. Owing to increase in use of these services by companies, several security issues have emerged and this challenges cloud computing architectures to secure, protect and process user's data. These services have certain cons like security, lock-in, lack of control, and reliability. Privacy and security are the major concerns in cloud computing services. In this paper, we have designed a novel secure framework for cloud services, as well as presented a critical analysis of CCMP (Counter with Cipher Block Message Authentication Code Protocol) protocol for secure data management of cloud services.

Keywords— Cloud Computing, Security, CCMP, Services

I. INTRODUCTION

Cloud computing is the Internet-based computing where the application software, infrastructure, and platform are exposed as software and the end users can access it through a distributed cloud, as a client. Cloud is a step on from utility computing and provides a convenient on demand network access to a shared pool of configurable computing and communication resources. Here, resources refer to computing applications, network resources, platforms, software services, virtual servers, and computing infrastructure [1]. Cloud computing is being widely adopted across many industrial sectors. Security, availability, and performance are the three biggest problems in cloud adoption. The serious challenge is how it reports security and privacy issues which occur due to movement of data and application on networks, loss of control on data, dissimilar nature of resources, and several security policies. Data storage, processing and movement outside the controls of an organization poses an inherent risk and making it vulnerable to various possible attacks. Cloud computing poses privacy concerns because the cloud service providers may access the data that is on the cloud that could accidentally or knowingly be changed or even removed, creating serious business trust and legal consequences [2].

Irrespective of employing framework having attributes for high reliability and availability, the services in cloud computing can experience denial of service attacks, performance slowdowns, equipment outages, and natural disasters. The level of reliability and availability of cloud resources must be considered as a serious problem into the organization's planning to set up the proper cloud infrastructure, providing effective services to consumers [3]. Therefore, resource management is an essential function of cloud infrastructure. It affects the three basic criteria for architecture evaluation of performance, functionality, and cost. Inefficient resource management has a direct negative impact on performance and cost. It can also indirectly affect system functionalities. A cloud infrastructure is a complicated architecture with a vast number of shared resources. These are subject to uncertain requests and can be influenced by external action beyond your control [6]. Cloud resource management requires complicated policies and decisions for multi-objective optimization. It is intensely challenging because of its distributed, heterogeneous, complex shape, which makes it impossible to have correct global state information. Therefore, there are various security concerns, namely: data security, data confidentiality, and compliance with government regulations, trust, identity management, architecture, software isolation and availability [4].

In this context, AES (Advanced Encryption Standard) is a candidate algorithm, since it is a very tough and non-breakable cipher by several attacks. According to the NIST specification, AES is capable of protecting sensitive government information well into the next century [8]. AES involves various rounds of length 10, 12 and 14 in the encryption process, as more rounds are involved in the transformation, the overall encryption strength increases. AES CCMP algorithm using 2-way interleaving that does not compromise the security of wireless communication sessions so we protects AAD (additional authenticated data) against replay attacks [8]. The AAD is derived from the MAC Protocol Data Unit (MPDU) header. It is 22–30 bytes in size. It is made from frame control, IP address of source, IP address of destination, MAC address of source and quality control [5]. Generally, the security is a joint responsibility of the cloud client and provider. However, the organization itself is

accountable for its all resources over the cloud. Although the cloud computing offers many benefits, for instance, low cost, data security and privacy issues pose serious concerns to this relationship among operators and users. This paper presents a novel privacy and security framework for the improvements of authentication and access control in the cloud services [7].

The remaining of the paper is organized as follows. The section II, presents a brief introduction about cloud services and their issues. The section III, presents a secure services framework for cloud network with respect to scalability and reliability. Section IV, presents secure cloud network for ITS. Section V, presents the performance analysis of CCMP protocol with AAD for ITS. Finally, we have concluded the paper in the section VI.

II. PERSPECTIVE AND CHALLENGES OF CLOUD SERVICE

Not only the collected cloud data need to be exposed to the software environment, but also the existent Cloud resources i.e. financial management, communications and collaboration, office productivity suits, accounting applications, customer relationship management, online storage management, human resource and employment or even entire cloud networks. In other words, Cloud resources need be exposed to software orchestration frameworks, allowing the dynamic and integrated composition of devices, networks, services, and applications. Entire service life-cycles can be orchestrated involving such exposed resources. First, services and applications can search for available Cloud devices. Second, dynamic usage contracts can be negotiated and established [7].

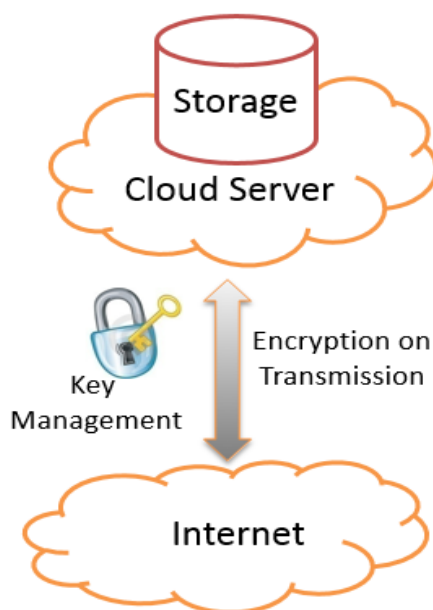


Figure 1. Encryption mechanism on cloud networks.

Nonetheless, Cloud capabilities can be seen as a service that is exposed to other software via orchestration frameworks and contracted on demand. This view approximates the Cloud to the so-called Internet of services. In this context, a first challenge is how to design a service oriented Cloud? A second

one is how to enable the joint orchestration of non-Cloud and Cloud substrate resources and services. The convergence, the search for synergies, and the elimination of redundant aspects in these two proposals, strengthen both and more efficiently addresses the challenges behind the design of convergent information architectures, which synergistically integrate information processing, exchanging, and storage [8].

The Cloud resources need to be very precisely exposed. Thus, device's descriptors can be elaborated and divulged to possible partners. The publish/subscribe paradigm fits very well on this task. Another very important challenge for cloud architectures is the consistent management of exposed resource life-cycle. In this context, some questions are: How to manage the life-cycle of exposed resources? How to share Cloud resources among several orchestration frameworks? How to describe the device capabilities? How to format the contracts? How to provide the adequate search mechanisms? Which circumstances can cause a contract revocation? These are open problems that need to be investigated [9].

III. PROPOSED FRAMEWORK FOR SECURE CLOUD NETWORK SERVICES

Figure 1 depicts the encryption mechanism of cloud server where data must be encrypted during communication between user (client) and cloud manager (server). Therefore, proxies can be used to represent simple networked objects that do not support such functionalities. We already know that CCM/CCMP is an amalgamation of two modes, the AES Counter Mode and the Cipher Block Chain MAC (CBC-MAC) mode [5]. The Counter Mode is used to perform encryption to guarantee data confidentiality. CBC-MAC is used to achieve data authenticity and integrity. Therefore, the proposed cloud frame work has used a two-pass authenticated encryption (AE) mode to perform an authentication in one cycle (client) and encryption in the second cycle (cloud-based server). In early generic-composed two-pass AE modes, two keys are used. One key is used for encryption to guarantee data confidentiality and the other key is used for authenticity and integrity. CCM/CCMP uses a single 128 bits key to achieve all three security goals of confidentiality, authenticity and integrity for cloud data management. Figure 2 depicts the necessary secure cloud infrastructure [4].

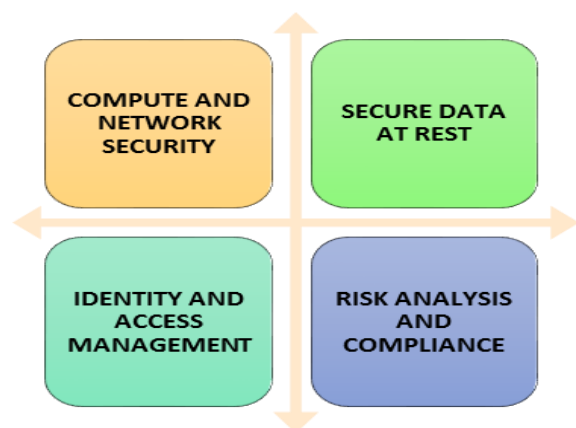


Figure 2 Security mechanism on cloud networks

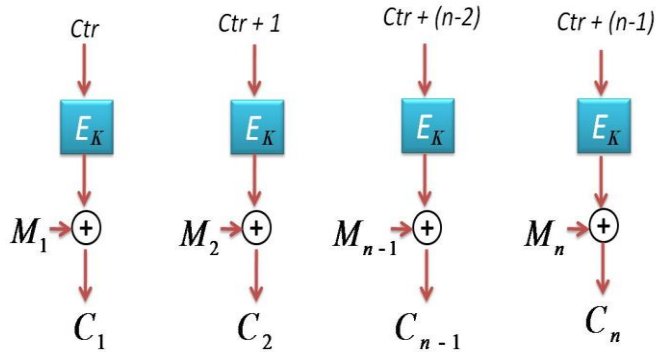


Figure 3. AES-CCMP counter mode encryption.

We have proposed a framework for cloud network services in the Figure 4 where three layers are presented from cloud computing to end-user. The communication layer contains a transportation stratum for sharing of information between end-user via an ad hoc network or to a cloud server in the event of an accident. In the transportation stratum, we have a Wi-Fi module and a Bluetooth module connected using their respective interfaces to the processor. Here, there are two processors for processing the data. First is the main processor and the second one is the subsidiary processor. The main processor will just share the data (video, audio, information about the location using GPS/Wi-Fi etc.) to the clients in the range of ad hoc network or to a cloud-based server using Internet services.

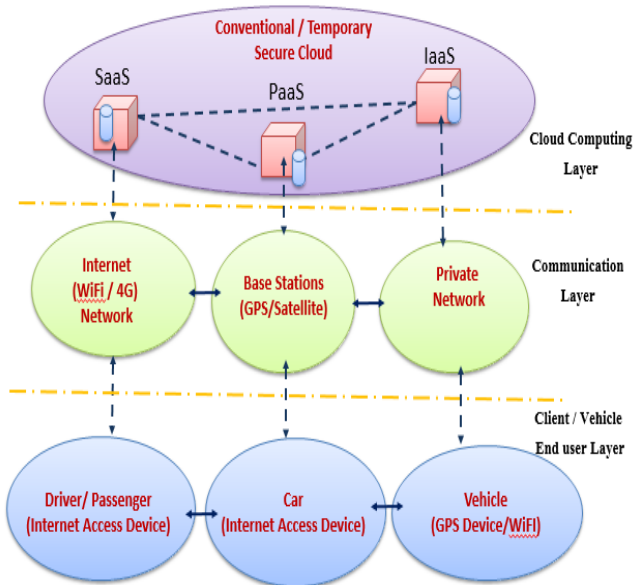


Figure 4. Proposed framework for cloud networks services.

The last part is the conventional cloud which is responsible of data collector stratum. It consists of various modules for collecting and transferring data and information like camera modules for rear and front, LCD module, GPS Module, pressure sensor for accident detection, temperature sensor for protecting the data which could be destroyed from excessive temperature, proximity sensor for vehicular lane change detection, and speed sensor.

IV. SECURE CLOUD NETWORKS FOR ITS

Cloud computing offers many benefits, scalable and flexibility to its end users. Users can operate from any place at any time in a secure way. With the increasing number of web-enabled devices used nowadays (e.g. tablets, smart phones, PC, Laptop etc.) access to one's information and data must be quick and easier by using above mentioned devices. The Counter Mode is used to perform encryption to guarantee data confidentiality. Following Rogaway and Wagner [10] for every MPDU encrypted, CCMP generates an additional 8 bytes CCMP header. The CCMP header is made of 48 bits nonce PN, 8 bits key ID, and 8 bits ext IV. CCMP also generates 30 bytes AAD from the MPDU header. In the scenario of Cloud services where Client to Server networking is required, the encryption key K lasts for a whole data communication session. Every session, a new encryption key requires a unique 13 bytes nonce value N for each MAC Protocol Data Unit (MPDU) encrypted. The nonce N ensures that the lifetime of encryption keys K are longer and that any replay attacks are detected and thwarted. N is constructed from the 48 bits packet number (PN), the 48 bits destination IP address (A2), and the 8 bits priority [8].

As an example, we are going to apply the aforementioned approach to an Intelligent Transportation System (ITS) based on cloud computing. Here, we can see that the information is collected using the collectors namely front and rear camera module for recording the pre and post-accident data. The information gathered is processed using a processor. The information is simultaneously sent to the end users who are nearby the ad-hoc network, without any intervention from third party electronics device so that they can receive the news about the nearby vehicles and the drivers can decide, whether to overtake the preceding cars or not. In the event of accident, the video recorded using the collectors and the information about the location specified by the GPS module are transferred to a Wi-Fi-based server so that the concerned authorities can have a look at the evidence stored. Figure 5 shows the transportation scenario where accident data is monitored by respective persons with the help of cloud networks.

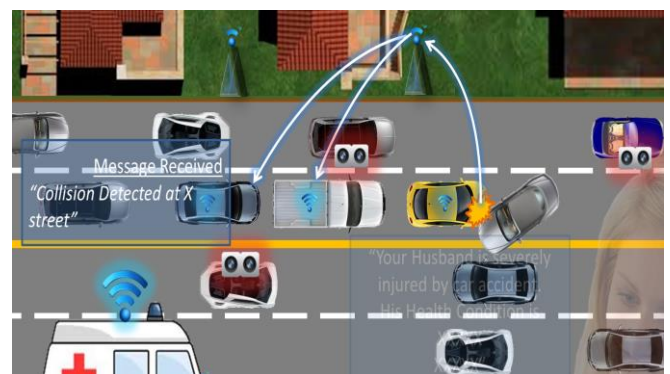


Figure 5. Cloud networks for intelligent transportation services.

In this cloud ITS service scenarios the AAD remains constant for the duration of an encryption data delivery session. CCMP should be able to pre-process the AAD just

once, at the beginning of the session after the first MPDU is processed. With this, all other subsequent MPDUs that follow will use the same AAD data to maintain efficiency. CCMP however fails to do this. CCMP has to re-process the AAD for every MPDU encrypted. This is because it computes the nonce N before the AAD rather than after it. Having established the desirability of an AE scheme like CCM/CCMP to be AEAD, the next step is to show how much efficiency is lost by CCM/CCMP for failing to pre-process the AAD. An MPDU varies in size between 1 to 2296 bytes. The number of MPDUs in any given payload greater than 2296 bytes ($M_P \geq 2296$) hereby referred to as MPDU_N is computed as shown in Equation (1).

$$\text{MPDU}_N = \left\lceil \frac{M_P}{2296} \right\rceil \quad (1)$$

We already know that the AAD is 30 bytes. This means for every 2296 bytes of payload that goes through the CCM originator processing, some excess data of at least 30 bytes has to be recalculated by the CCM/CCMP authenticated encryption process.

An MPDU may however be far less than the 2296 bytes. Regardless, the problem of CCMP not being able to pre-process AAD will still manifest itself as 30 bytes of AAD has to be generated for every MPDU encrypted. For any given size of plaintext payload ≥ 2296 bytes encrypted, the minimum amount of excess AAD hereby referred to as AAD_{Min} is computed in equation (2).

$$\text{AAD}_{\text{Min}} = \left\lceil \frac{M_P}{2296} + 1 \right\rceil * 30 \text{ bytes} \quad (2)$$

Equipped with the minimum amount of excess AAD generated from any payload ≥ 2296 bytes, a table and graph is produced, which shows how much efficiency is lost by CCM/CCMP for having to re-compute this surplus AAD. Equation (3) shows the computation for plaintext payload with excess AAD hereby referred to as P_{+AAD} .

$$P_{+AAD} = M_P + \left(\left\lceil \frac{M_P}{2296} + 1 \right\rceil * 30 \text{ bytes} \right) \quad (3)$$

Table 1 below shows the relationship between payload with excess AAD and payload without excess AAD. The table is computed for payload varying between 1Megabytes to 100 Megabytes.

TABLE 1. COMPUTING CCMP PAYLOAD WITH EXCESS AAD, AND WITHOUT EXCESS AAD.

$M_P = \text{Payload}$	1024 000 bytes	5120 000 bytes	10240 000 bytes	512000 00 bytes	102400 000 bytes
AAD	30 bytes	30 bytes	30 bytes	30 bytes	30 bytes

Payload without excess AAD $P_{-AAD} = M_P + \text{AAD}$	1024 030 bytes	5120 030 bytes	10240 000 bytes	512000 30 bytes	102400 030 bytes
Payload including excess AAD $[P_{+AAD} = (3)]$	1037 410 bytes	5186 929 bytes	10373 828 bytes	518690 20 bytes	103738 009 bytes

Having established a link between CCM/CCMP payload with excess AAD and payload without excess AAD from Table 1.

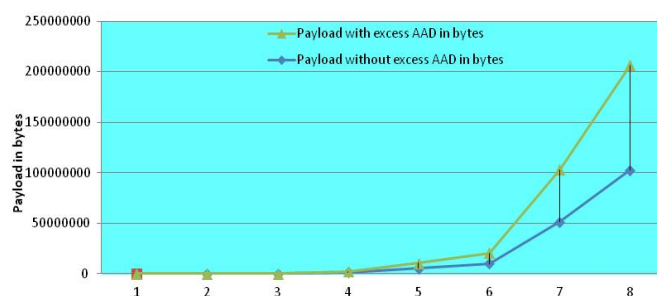


Figure 6. CCMP Payload with excess AAD, and without excess AAD.

Figure 6 shows the trajectory path of difference in efficiency between the two scenarios and the comparison between payloads with excess AAD overhead against the original payload without excess AAD. For any 102,400,030 bytes of data processed, the excess AAD is (103,738,009–102,400,030) bytes=1,337,979 bytes. This is unnecessary waste of computing time and processing power [5].

V. CONCLUSION

There are several advantages of cloud computing such as high level computing, scalability and pay-as-you use. Cloud service provider has less transparency than other information security policy. As a result, it may create clash with the enterprise's information. The enterprise needs to have detailed understanding of the service level agreements that requires desired level of security provided by the cloud service and cloud networks must enhanced the performance when a user moves to cloud computing infrastructure. The computing performance is normally measured by capabilities of applications running on the cloud system. However, this paper discusses the insight computing of CCMP payload with excess AAD, and without excess AAD and designed a novel secure framework for cloud services, as well as presented a critical analysis of CCMP protocol for secure data management of cloud network ITS services. We present a novel privacy and security scenario user and cloud network management ITS services.

ACKNOWLEDGEMENTS

This work was supported by Hankuk University of Foreign Studies South Korea fund 2015 and University of Applied Sciences Western Switzerland (HES-SO), the Swiss national government through the Sciex-NMSch (Scientific Exchange

Programme between Switzerland and the New Member States of the EU) with the project code 13.121, named BASTION "Bootstrapping, Authentication, Security and Trust for the Internet of Things Networks". The authors would like to thank also projects SAFESSENS ENIAC Joint Undertaking with the Grant Agreement no: 621272, and the EU Horizon 2020 projects ENTROPY with the Grant Agreement no: 649849 and INPUT with the Grant Agreement no: 644672.

REFERENCES

- [1] M. Hogan, F. Liu, A. Sokol, J. Tong, NIST Cloud Computing Standards Roadmap – Version 1.0, Natl. Inst. Stand. Technol. Spec. Publ. 500-291, 83 pages, July 5, 2011.
- [2] R. Ahuja "SLA Based Scheduler for Cloud storage and Computational Services", International Conference on Computational Science and Applications (ICCSA), pp.258-262, June 2011.
- [3] A. Albeshri W. Caelli, "Mutual Protection in a Cloud Computing Environment", 12th IEEE International Conference on High performance Computing and Communications (HPCC), pp. 641-646, Sept 2010.
- [4] S. Almulalla, Y-Y Chon, "Cloud Computing Security management", 2nd International Conference On Engineering Systems Management and Its Applications, pp.1-7, March 2010.
- [5] I. Ahmed, A. James, D. Singh, "Critical analysis of counter mode with cipher block chain message authentication mode protocol—CCMP", *Security and Communication Networks*, Volume 7, Issue 2, pages 293–308, February 2014.
- [6] Security Guide for Critical Area s of Focus in Cloud Computing V3.0 <https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>
- [7] F. Khodadadi, R.N. Calheiros, R. Buyya, "A Data-Centric Framework for Development and Deployment of Internet of Things Applications in Clouds", *Proc. of the 10th IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP 2015)*, Singapore, April 7-9, 2015.
- [8] Z. Codabux-Rossan, M R. Doomun, "AES CCMP Algorithm with □-Way Interleaved Cipher Block Chaining", *University of Mauritius Research Journal*, Vol. 15, pp. 527-544, 2009



Irish Singh is doing M. Tech in Computer Science and Engineering from Birla Institute of Technology, Ranchi (Allahabad campus). She did her B. Tech in Computer Science and Engineering from U P (State) Technical University, Lucknow, India. Her fields of research interests are Security issue in Big Data, Cloud computing, ICN and IoT.



Kamta Nath Mishra received his Master of Technology degree in Software Systems from Birla Institute of Technology and Science (BITS) Pilani, INDIA in 2003, He is an Assistant professor at Birla Institute of Technology, Mesra, Ranchi, INDIA (Allahabad Campus) and pursuing Ph.D. from the same Institute. Previously, Mr. Mishra worked with Sebha University, Libya, B.I.T. Noida, CDAC Noida, and K.I.E.T. Ghaziabad before joining B.I.T. Allahabad campus. His research interest includes Biometric systems Based Personal Identification Methods, Image Processing and Analysis of Algorithms.



Antonio M. Alberti received the degree in Electrical Engineering from Santa Maria Federal University (UFSM), Santa Maria, Brazil, in 1986, and the M.Sc. and Ph.D. degrees in Electrical Engineering from Campinas State University (Unicamp), Campinas, SP, Brazil, in 1998 and 2003, respectively. In Feb. 2004, he joined as an Adjunct Professor at National Institute of Telecommunications (INATEL), Brazil. His field of research interests are Future Internet, Future ICT & Artificial Intelligence.



Antonio J. Jara, Assistant Prof. PostDoc at (HES-SO) Switzerland, Vice-chair of the IEEE Communications Society Internet of Things Technical Committee, and founder of HOP Ubiquitous S.L., He did his PhD (Cum Laude) at the Intelligent Systems and Telematics Research Group of the University of Murcia (UMU), Spain. He received two M.S. (Hons. - valedictorian) degrees. He has published 100+ international papers with a patent. Since 2007, he has participated into the several projects about the IPv6, Internet of Things, Smart Cities, and mobile healthcare.



Dhananjay Singh (SM 14) received his M Tech. in IT from IIIT-Allahabad in 2006 and PhD in IT from DSU-Korea in 2010. After that he has worked at NIMS and ETRI, Korea 2010-2012. In Sept. 2012, he joined as an Asst. Prof. in the Dept. of Electronics Engineering at Hankuk University of Foreign Studies, Korea. He has published 75+ referred scientific papers, delivered 25+ invited talks and serve 10+ editorial board and 50+ TPC membership. He is a senior member of IEEE.