ARCHITECTURE INTEROPERABILITY BETWEEN CLOUD COMPUTING AND NAMED DATA NETWORKING: SECURITY ISSUES ON REVIEW

[1]Sulaiman Yakubu Yunus, [2]Umar Abubakar Abdullahi and [3]Magaji Yunusa Rabi'u

[1]Computer Science Department, Audu Bako College of Agriculture Danbatta-Kano

[2]Computer Engineering Department, Kano State Polytechnic-Kano,
abubakartofa@gmail.com

[3]Electrical Engineering Department, Kano State Polytechnic-Kano,
yunusarabiumagaji@gmail.com

Corresponding author: yakubuy10@gmail.com, 07069211304

Abstract:

The development and implementation of cloud applications and services in the internet is increasing from all directions ranging from banking, education, businesses, healthcare and other aspects of human endeavor due to effectiveness, efficiency, reliability, and cost management. It now becomes an acceptable technology for ubiquitous computing activities around the globe, both by users and the cloud service providers (CSPs) like Amazon, Google, and Microsoft providing computing services via the internet, based on demand and pay per use. The cloud architecture now becomes an important concern for the cloud environment to maintain its robustness and ubiquitous contents accommodation and delivery as needed. This is why the need of information-centric networking architecture arises; where the content delivery can be carried out with minimal number of infrastructures (like storage capacity, bandwidth, and throughput), due to logical caching system. Although, today's internet cache data by the use of proxy (either free or licensed one) and browsers automatic caching, and this is associated with cost and security vulnerability. Therefore, adopting Named Data Networking (NDN) architecture will reduce the major challenges with cloud services, because NDN architecture aimed at securing the data first and allowed automatic caching of data at transit. That is why, this paper explore, survey and suggest the NDN architecture to replace IP (internet protocol) - based architecture for cloud computing environment to optimize the storage capacity and data security.

Keywords: Cloud computing, Named Data Networking (NDN), security issues, caching, Internet protocol (IP), Future Internet Architecture (FIA).

1.0 Introduction:

There is no doubt; cloud computing environment depends heavily on the core internet architecture, where the cloud applications, infrastructure and services are hosted and access via the internet [6]. It is the current computing direction for internet-base technology supporting various network entities; both cloud service providers (Amazon, IBM, Microsoft, and Google e.t.c.) and their clients for business association. This architecture provides computing services via the internet on demand and pay per used access to a pool of shared resources namely networks, storage space, servers, services and applications without physically acquiring them [2]. The cloud technology popularity was a result of emergence of large, small and medium enterprises, in order to cut-down cost, flexibility, efficiency of service delivery and an opportunity to participate in the global market [1]. The cloud services and applications enable users to store and access their local data in the remote data center by using their personal computers, or mobile devices; making the cloud to experience serious challenges ranging from servers, security issues regarding the data and communication channels. Although, the cloud vendors are employing the virtualization techniques to enable the sharing of computing resources in order to improves the utilization of cloud property [6].

However, considering the major challenges experienced by cloud architecture in terms of data security management like; data transmission, privacy, integrity, availability and network security in general, there is need of security-tolerance platform for conveniences and truth in using cloud services [7]. On the other hand, Named Data Networking (NDN) architecture was proposed to address some of the shortcomings with current internet architecture intended to make the cloud a more secured information-centric network. The NDN network prioritized securing the data first by encrypting the data rather its location/host or the transmission medium to avoid illegitimate access to data within the cloud environment, as in the case of today's architecture where the cloud vendors secure the data location and communication paths [3].

Therefore, this paper will describe the architectural stand of both cloud computing and NDN with their security models in the first section. In the second segment, the paper will outline the security comparison while the paper will lastly conclude with recommendation of cloud architecture to adopt the implementation of NDN in deploying cloud services.

1.1 Cloud Computing Architecture:

According to World Scientific News (WSN) [15] *"Cloud Computing is a model for enabling ubiquitous, convenient on demand access to a shared pool of configurable computing resources (e.g., network servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction",* that is characterized by shared infrastructure and dynamic provisioning of network services via computing devices such as laptops computer, tablets and mobile devices [2] by different cloud users. The cloud is completely internet dependent technology where client data is stored and maintain in the data center of cloud provider (internet service providers-ISP, telecommunication companies and large businesses) [7]. As a result of this, cloud

environment requires careful attention to make the data safe and confidential across the platform, which can encapsulate within the cloud models.

1.2 Cloud Computing Models:

The cloud models serve as the fundamental designing principles governing the operation of cloud activities, which includes software as a service (SaaS), Infrastructure as a Service (Iaas) and Platform as a Service (Paas), where the services are created, maintained and accessed when the need arises. This is explained and illustrated in figure 1 below;

I. Software as a Service (SaaS): it can be describe as a process in which cloud service providers provide software applications over the internet via a simple browser, so that the clients can easily access and install with less control and maintenance cost. SaaS vendors take full control of managing middleware, hardware or the operating system enabling the customers to benefit from updates on every technology subscribed by the users [15]. Example of Information Technology (IT) companies providing SaaS services includes; salesforce.com and Google apps

II. **Platform as a Service (PaaS):** PaaS is the deployment and delivery of computing platform without the cost of managing software and hardware. Appalications or services in PaaS are independent of the platform running the services, so the customers can use freely as needed. Example of PaaS includes; Microsoft Azure and Google App Engine where a developer can install and customize their applications using python language [11].

III. **Infrastructure as a Service (IaaS):** IaaS refers to the sharing of hardware resources for executing services using Virtualization technology [6]. Virtualization allows the distribution and separation of computing resources, and is a core machinery of cloud computing by running various virtual equipments. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Amazon's Elastic Compute Cloud is one common example of IaaS.

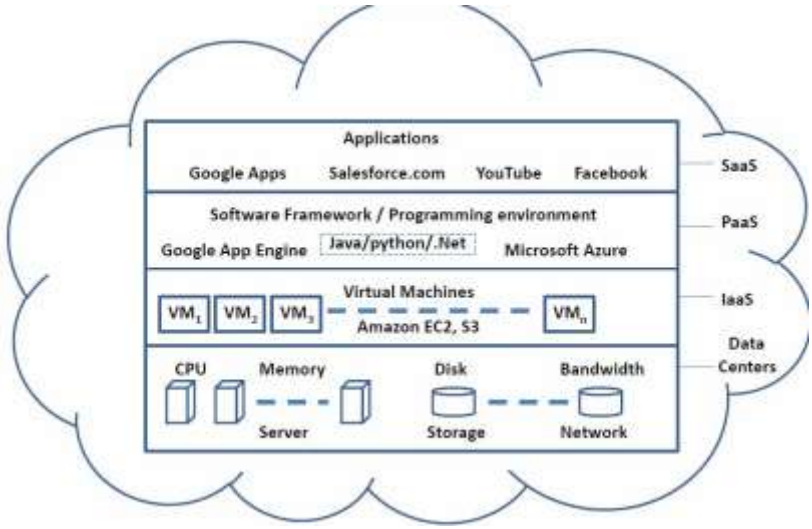

Figure 1: Cloud Computing Architecture-[7]

1.3 Security in Cloud Computing:

Cloud security is an important concern to every user within cloud environment, due to the voluminous and sensitivity of data across the cloud infrastructure, applications, and platform; being it public, private or hybrid nature of the computing services [11]. As stated by [1] the designing and implementation of cloud computing services is a constituting factor for further adoption of cloud manufacturing and businesses, for the noticeable experiences by high content distribution spreading all over the internet. This cloud development was encountered due to availability of desired content, easy access to the content, and cost management per service use [3]. Therefore, because of this internet revolution, the cloud is experiencing some security challenges such as; network security, data security (availability, its transmission, privacy, integrity), denial of service and virtual machine attacks e.t.c. [3, 11 & 7].

However, the cloud need to be protected, because the devices used to provide the services do not belongs to the users, and they have no control or knowledge about what will happen to the data being stored on cloud [8]. That is why! Cloud users used ask questions like;

- How secured is the cloud?
- Can unauthorized user gain access to confidential data?

Therefore, the cloud vendors, the users and internet developers are collaborative tasks to ensure the security of the environment, as stated by [12]; some decades back IPv6 protocol in TCP/IP architecture was introduced to replace IPv4 in order to solve some security problems with today's internet to suit with cloud activities.

Countermeasures: the security issues in cloud computing are particularly found at service provider layer, virtual machine layer and data center layer whose targeting IaaS as shown in Figure 2 below. A lot of researches have been done and a lot are in progress to overcome the security challenges associated with the cloud; for instance [6] emphasized that the data can be secure by ensuring and implementing appropriate policy and algorithm for the data to be digitally and cryptographically encrypt the cloud data for integrity, confidentiality and availability. Another important issue is the security of Domain Name System (DNS) where translation of domain name to IP address is taking place. While in [7] the Domain Name System Security Extension (DNSSEC) introduced to reduces the effect of DNS threats, but yet the attacks on transmission (between sender and receiver) medium remain unknown.

More importantly, the data security depends on the type of encryption/decryption algorithm used in securing the data; as in [8] & [7] Secret Socket Layer (SSL) encryption was suggested to protect the data symmetrically. In addition to [8] Amazon web services encourages users to encrypt sensitive data using TrueCrypt software free software for encrypting data before it is send to the cloud devices. Another authors suggest that data should be protected at stages (at rest or in transit) [9] for the data to be preserve its confidentiality, integrity and availability. This paper also employs the use of popular symmetric encryption algorithm like Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA).

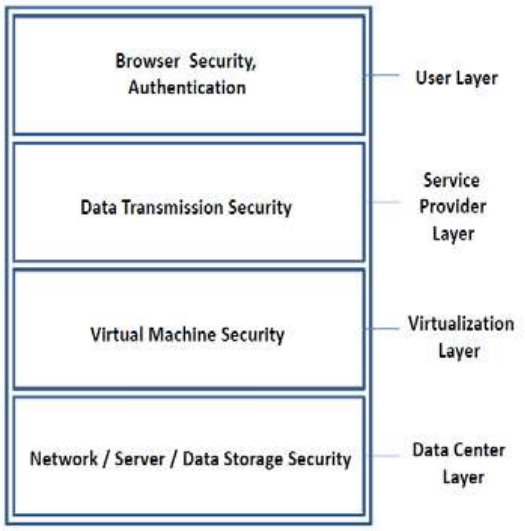

Figure 2: Security Architecture in Cloud Computing -[7]

2.1 Named Data Networking (NDN) Architecture:

NDN architecture is one of the proposed Future Internet Architecture based on information-centric network focuses on replacing today's IP addresses by naming data directly in order to build distributed network of applications [5] without considering data location or where it follows between a sender and the receiver. NDN was proposed to address some of the shortcomings of the current internet architecture, that can facilitates content distribution and delivery with better communication model for scalability and security of data, between individual users connected to Internet. Because, today's internet is experiencing global challenge of resources management, allocation, and transmission [4] due to increase in extensive use of internet services for daily activities. The data prioritization in NDN architecture comes along with; improved data security, built-in caching and scalable routing, content distribution, truth verification by data receiver- it allows every node to verify the data before making copy, forwarding adaptability, and network address space minimization by implementing hierarchical naming structures that give unbounded namespace [3]. NDN evolved to maintain the hourglass shape of today's internet by including named data instead of location at its thin waist, that brings efficient and secured data retrieval due to digital signing of all chunk of data from origin to avoid further middleware configuration between network layer and application layer as illustrated in figure 3 below.

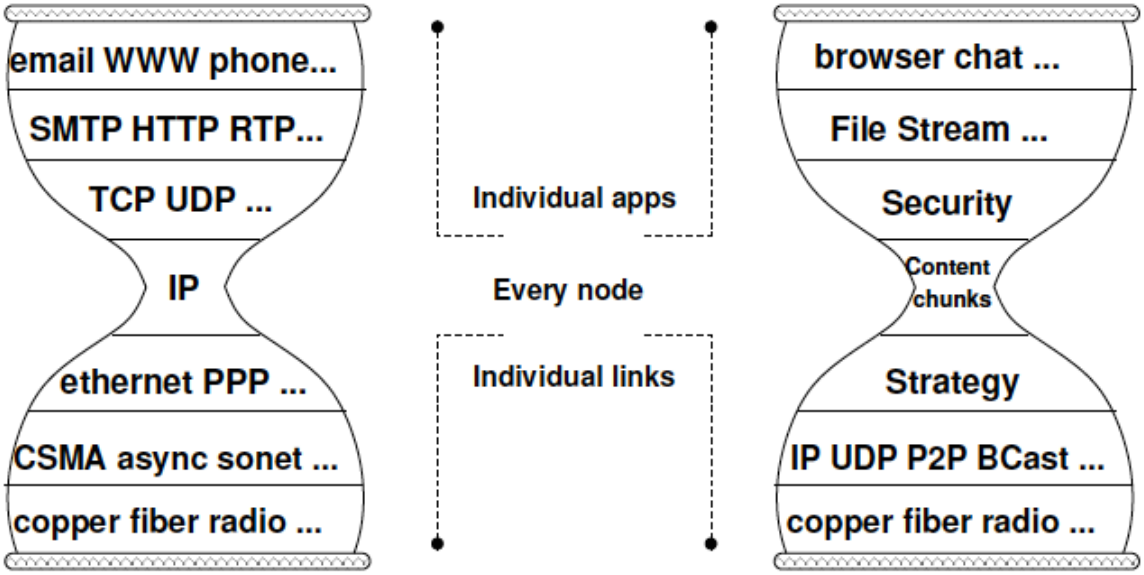

Figure 3: Architectural Transition from IP to NDN-[12]

2.2 NDN Components:

The routing, forwarding and caching of data in NDN is done within every router's control plane containing three tables; Content Store (CS), Pending Interest Table (PIT) and Forwarding Information Base (FIB) as stated by [14].

- Content Store (CS); is the route's buffer memory, where cached data is stored for a period of time, it serve future request of consumers with the available data, to reduce user's latency and save network bandwidth.

- Pending Interest Table (PIT):

  This is a table containing name prefixes of unsatisfied arrival interest and corresponding incoming interfaces. PIT entry records the interest name, the incoming interface (s) of the interest and the outgoing interfaces which the interest can be forwarded for retrieving data packet, based on FIB's longest prefix match. The entries are removed from the PIT after the lifetime assigned to it expires without data packet returns, so that it is left to the consumer to retransmit again, in order to reduce PIT explosion. PIT avoid forwarding of request with the same content name, the router only appends interface of the new request having the same name with the one already forwarded. PIT is responsible for data multicasting delivery based on its entries, because multiple entries with the same request can be serving at the same time. It

initiates and coordinates the routing of interest packet without specifying a source or destination address.

- Forwarding Information Base (FIB):

  Is a table of name prefixes and corresponding outgoing interfaces, in order to route interest to the matching data packet. It contains multiple interfaces to forward different consumers' request. It decides where and what are the longest prefix matches for interest packet to follow. NDN FIB differs from IP FIB in two ways;

  I- NDN FIB contains multiple forwarding interfaces for next-hop count while that of IP contain single next-hop.

  II- IP FIB contains next-hop information only while NDN FIB contains information both from routing and forwarding plane to provide better forwarding decision based on the updated network information to avoid following failed link.

2.3 NDN Operation:

NDN is user-driven communication network based on two types of packets; interest packet and data packet; interest packet is a user request for a particular data in the network while data packet is the corresponding data in return from a content server or any node with matching requested interest. In which a consumer sends out an interest packet throughout the network which carries the name of content identifying a block of data in order to get the desired data packet, without knowledge about the content producer, because NDN client believe that the request can be satisfied from any node within the network [12]. Any router having the matched data will respond to it by sending the data packet along the same way the interest passed, because an NDN interest request always leave a trail trace during the forwarding process, so that a symmetric routing is made between the two packets from the requester to the content producer or any node satisfying the interest [10]. Every interest packet is always satisfied with corresponding name prefix in the content name in the data packet.

The NDN interest and data packet are entirely different from IP packet not only considering the replacement of addresses with named data, but there are some special fields attached to both interest and data packet which brings uniqueness and security issue to both consumers and producers. For example, the figure below shows the content of interest and data packet with all the necessary part.

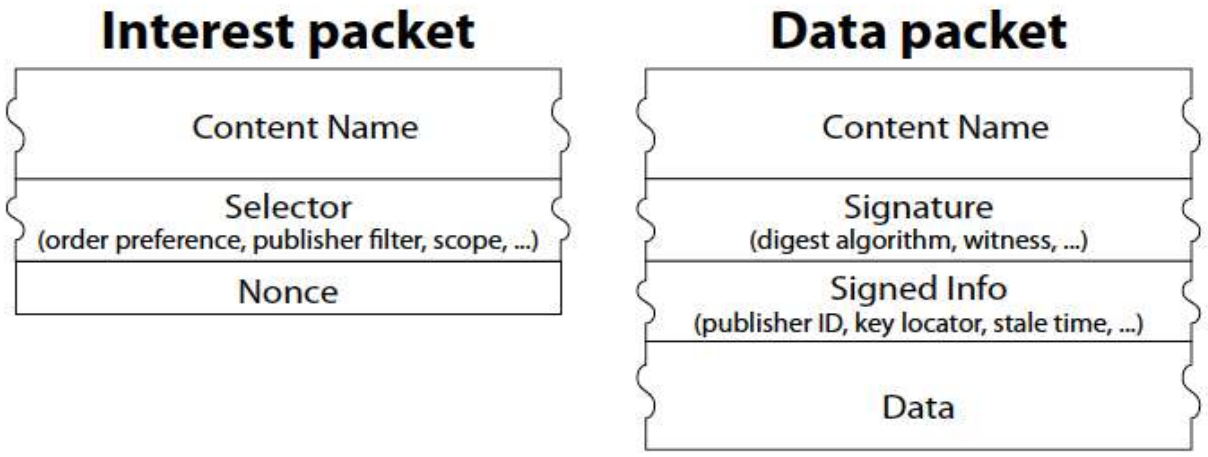

Figure 4: NDN Packets-[12]

2.4 Security in NDN:

NDN is a content-based security that provides authentication and digital signature for each data, because securing the network content is much more important than securing the endpoints [12]. Beside automatic data protection, NDN have improved some of the security measure with today's internet and introduced others. For example, [13] presented comparative possible attacks between NDN and TCP/IP network; as mentioned, NDN is free of bandwidth depletion attack, reflection attack, black-holing and prefix hijacking, but it is associated with other types of Denial of Service (DoS) attacks such as interest flooding and content/cache poisoning (CP) and pollution attack e.t.c. Interest Flooding (IF) is the ability of adversary/attacker to flood the PIT with illegitimate interest to block the incoming legitimate packet from reaching the router while cache poisoning allows the adversary to insert corrupted entries in a DNS server in order to control the server responses.

NDN control the first (IF) through the use of NDN DNS, which shows successful implementation of DNSSEC protocol with complete nature of content distribution networks [13] & [16]. While, the second attack (CP) can be tackle using router's information by; router statistics and push back mechanisms. Another countermeasure for pollution attack, is by using Cacheshield technique, in which NDN improve cache robustness by caching non popular content with any replacement policy, although the author tailored some draw backs associated with it. The most concern security issues in NDN depends on the encryption/decryption algorithm for every data chunk, as in [12] where a comparison of RSA and Elliptic Curve Digital Signature (ECDSA) were carried out for secret key generation per second for the equivalent public, as shown in the two tables below. Remember both RSA and ECDSA are asymmetric algorithm that use pair of keys; public key and private key (secret key) for data encryption/decryption which is more secure than symmetric that use single key for encryption and decryption like AES, CAT5, TwoFish e.t.c.

Key length	RSA-512	RSA-1024	RSA-2048	RSA-4096
Key generator (sec)	0.112	0.232	1.322	1.112

Table 1: RSA key generator-[12]

Key length bits	ECDSA 160	ECDSA 190	ECDSA 224	ECDSA 256	ECDSA 384	ECDSA 512
Key generator (sec)	0.0151	0.155	0.219	0.303	0.621	1.573

Table 2: ECDSA key generator-[12]

Based on the table above RSA has larger key size than ECDSA, and it provide better security but takes more for the encryption and decryption, that lead to another security challenge, there by declaring ECDSA the best for fast encryption/decryption.

3.0 Comparison between NDN and Cloud Computing

In contrast, NDN and IP architecture share a similar structure of hourglass with narrow waist as shown in figure 3 above, but the IP packets in the narrow waist was replace with NDN packets. And also, IP routers are stateless, they do not store any information about the processed packets while NDN routers are stateful so that requested packets are cached in CS in order to serve future request. In case of security, IP network security is implemented via end-to-end channel while NDN secure the data from its origin [4] & [12], as it shows in figure 5 below. Moreover, for trust management NDN are using conventional and distributed naming system, where every entity must have an identity (namespace) and the corresponding certificate for this namespace, because NDN name should share the same prefix with the corresponding data. For example /NDN/cnnNews/ is a prefix to /NDN/cnnNews/ EgyptCrisis/2013 and the match [16]

Therefore, the security compatibility proposed in this paper was based on the above hypothesis where

I- Cloud computing robustness requires content centric and distribution architecture, which is one of the fundamental principles of NDN architecture.

II- Cloud computing are experiencing more security challenges concerning the data confidentiality, privacy, integrity, authentication e.t.c. and the network services in general, while NDN emphasized and prioritized securing data from its origin using the high quality encryption/decryption techniques like RSA and ECDSA.

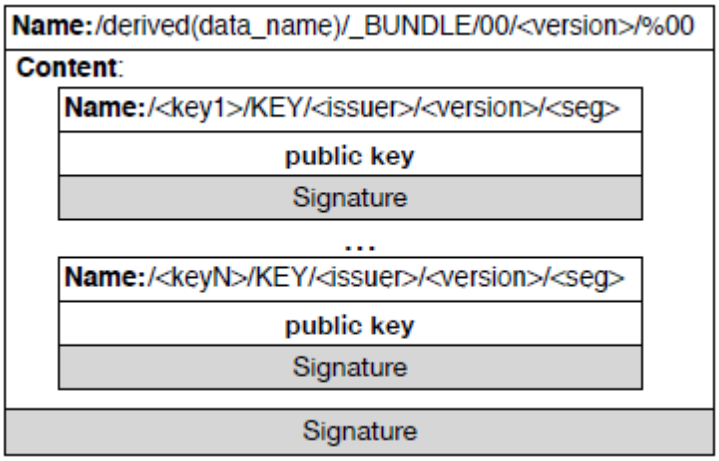

Figure 5: Data Packet Key Bundling-[4]

4.0 Conclusion:

Considering the comparative analysis lamented in this paper between cloud computing (IP-based architecture) and NDN network, it is cleared that NDN implementation can overcome most of the challenges with today's cloud environment, particularly the security issues and storage optimization, because NDN was selected by National Science Foundation (NFS) since 2010 supported by other European University like UCLA, ARIZON, COLARADO State University and others, among the proposed Future Internet Architecture (FIA). Other FIA includes Nebula, MobiliFirst, and Expressive Internet Architecture e.t.c. Therefore, this paper is concluded with suggestion from internet based researchers to continue taking NDN to the next phase of implementation.

References:

[1] Mourtzis, D., Schoinochoritis, B., & Vlachou, K. (2015). A New Era of Web Collaboration : Cloud Computing and its Applications in Manufacturing. *Conference: 8th IWC Total Quality Management Advanced and Intelligent Approaches*, (September).

[2] Manzoor, D., Ali, A., & Ahmad, A. (2014). Cloud and Web Technologies : Technical Improvements and Their Implications on E- Governance. *International Journal of Advanced Computer Science and Applications*, *5*(5), 196–201.

[3] Shang, W., Wang, Z., Afanasyev, A., Burke, J., & Zhang, L. (2017). Breaking out of the Cloud. *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation - IoTDI '17*, 3–13. https://doi.org/10.1145/3054977.3054993

[4] Partridge, C., Nelson, S., & Kong, D. (2017). Realizing a virtual private network using named data networking. *Proceedings of ACM ICN*, 156–162. https://doi.org/10.1145/3125719.3125720

[5] Conti, M., Gasti, P., & Teoli, M. (2013). A lightweight mechanism for detection of cache pollution attacks in Named Data Networking. *Computer Networks*, *57*(16), 3178–3191. https://doi.org/10.1016/j.comnet.2013.07.034

[6] Bunkar, R. & Rai P.K. (2017). Study on Security Model in Cloud, (August). https://doi.org/10.26483/ijarcs.v8i7.4350

[7] Padhy, R., Patra, M., & Satapathy, S. (2011). Cloud Computing: Security Issues and Research Challenges. *... Information Technology & Security ...*, *1*(2), 136–146. Retrieved from http://ijcsits.org/papers/Vol1no22011/13vol1no2.pdf

[8] Mohamed, E. M. Abdelkader, H.S. and El-Etriby, S. (2013). Data security model for cloud computing. Department of Computer Science, Faculty of Computers and Information, Menofia University, Menofia 32511, Egypt 23–43. 31/9/2013 https://www.researchgate.net/publication/264235525

[9] Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. *Procedia Computer Science*, *125*(2009), 691–697. https://doi.org/10.1016/j.procs.2017.12.089

[10] Tsudik, G. (2017). Security & Privacy in Content-Centric Networking. University of Carlifornia, Irvine (UCL). 8//2012.1–44.

[11] Wanjira, M.J. (2016). A Data Security Implementation Model For Cloud Computing In Government Parastatals. School Of Computing And Informatics Research Project Report, University Of Nairobi, August 2016, 89680–89684.

[12] Foushanji, P. (2017) Evaluation of RSA and ECDSA Applying for Information Centric Networking. Department of Computer Sceince and Communication Engineering. Waseda University Graduate School of Fundamental Science & Engineering. 30/1/2017. 1–38.

[13] Gasti, P., Tsudik, G., Uzun, E., & Zhang, L. (2012). DoS and DDoS in Named-Data Networking. Retrieved from http://arxiv.org/abs/1208.0952

[14] Sifalakis, M., Kohler, B., Christopher, C., & Tschudin, C. (2014). An information centric network for computing the distribution of computations. *Proceedings of the 1st International Conference on Information-Centric Networking - INC '14*, 137–146. https://doi.org/10.1145/2660129.2660150

[15] Alam, S. Bin. (2017). Cloud Computing – Architecture , Platform and Security Issues : A Survey. *World Scientfic News*, *86*(3), 253–264.

[16] Jacobson, V., Burke, J., Zhang, L., Abdelzaher, T., Zhang, B., Claffy, K., … Wang, L. (2016). Named Data Networking Next Phase (NDN-NP) Project Annual Report Principal Investigators, (April). Retrieved from https://www.caida.org/publications/papers/2017/named_data_networking_2016-2017/named_data_networking_2016-2017.pdf