Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 4, April -2016

Current Internet Architecture Comparison with NDN based on TCP/IP

Rajeev Goyal

Assistant Professor, Dept. of CSE, Amity University, Gwalior

ABSTRACT:-Over time number of people using internet has escalated. The primary reason of the internet has been revised. To deal with this drastic trade, network architecture has to be redesigned thinking about future developments. The future architecture of internet can be advanced best after scrutinizing numerous points of present day internet architecture. For this reason observe of strengths and weaknesses of existing architecture will guide the freshmen to build a strong future architecture of internet. This paper represents comparative take a look at of TCP/IP version of current architecture and Name Data networking (NDN) method of content Centric networking of proposed model. This paper discusses fundamental points including processes to current and future architectural version, Packet formats and differences in security mechanisms of these models.

***Keywords :-** Named Data Network, Content Centric Networks, Future Internet Architecture, Network Architecture and Design.*

1. INTRODUCTION

First of all, when evolution in computing had begun computing resources had been confined. Use of computer systems turned into limited to high priority military operations and research institutions. Computing resources together with tape drives, storage disks or non computing sources like information documents, scientific findings and research papers frequently had to be shared. So as to percentage such resources, communication between the two computing machines turned into information. With this objective a complex network of computers placed throughout different geographic locations changed into evolved. Achievement of sharing the data using a network of computer systems and ease of access computing resources endorsed the colleges and company groups to expand their very own networks. These heterogeneous bodily networks ought to talk with each different the usage of the TCP/IP. Inter-connection of these networks results in the invention of the internet.

Using net has appreciably changed from mere communication to data dissemination. Staggering quantity of data is generated every day. Human beings are using net to save their content on-line on the way to access their content from everywhere in the international. Humans use internet to discover information about jobs vacancies, news articles, work related data, on line tutorials and many others in text, video or audio formats. A latest article in Forbes sheds mild on how the popularity collection “Game of Thrones” was downloaded 1.5 million times. Which cause switch of 2,000 terabytes of data inside 12 hours after its telecast? It’s far a known reality that

Once a video is going viral, it gets massive wide variety of requests from different parts of the world concurrently. On the way to satisfy such excessive wide variety of requests concurrently, implementation of latest multicast algorithms is required. NDN architecture handles such conditions correctly as it is multipoint to multipoint protocol unlike TCP/IP. Net model of TCP/IP is based on the verbal exchange between machines. This verbal exchange requires addresses of source and destination gadget. Today’s internet version isn't best suited for data dissemination. The proposed version of NDN is applied the use of content Centric Networking technique. On this architecture the content is named. The objective of NDN architecture is to efficiently manage the issues that contemporary net architecture faces. This future architecture guarantees better usage of bandwidth, aims to improve throughput and reduce the network traffic generated all through the transfer of popular net content. On this paper detail comparison of existing TCP/IP model and proposed NDN model is given.

This paper wills resource the reader to recognize essential variations between present day net architecture and future internet architecture. This Paper represents a comparison of architectures in a simplified manner. It includes simple functioning methods and architectural components of each the systems. It emphasizes on distinguishing elements among TCP/IP and NDN version. Packet formats and security implementations also are mentioned on this paper. By the end of this paper reader could have clear information of how these architectures vary.

2. COMPARITIVE STUDY

NDN	TCP/IP
Future Internet Architecture	Current Internet Architecture
Information Distribution	Information Sharing
Information Centric Network	Conversation Oriented
Content Centric	Address Centric
Elimination of DNS	Can’t Function without DNS
Not Host Centric	Host Centric
Multipoint to Multipoint	Point to Point
Large Scale Information Dissemination	Inefficient Information Dissemination
Router Content Cache	No Router
In-Network Storage	Content Cache No In-Network Storage
Optimization of Bandwidth Congestion Reduction Improved throughput	No Optimization of Bandwidth Often Congestion Occurs
Tasteful Data Plane, Adaptive Forwarding	Stateless Data Plane Non Adaptive Forwarding by Router
3 Entities Maintained	1 Entity
FIB, PIT, CS	FIB
FIB Stores Multiple Hop Status, Performance Information	FIB Stores Only Next Hop Information
Existing Routing Protocols Propagation based On Name Prefix	Existing Routing Protocols Propagation Based on IP prefix
Security is Provided to Content Itself Not Using Abstractions	End to End Channel is Secured like SSL
Interest Initiated Model	Client Server Model for Interaction

Content Distribution (many users REQUESTING SAME DATA AT DIFFERENT TIME) , Multicast(SAME TIME) both Handled efficiently	Inefficient Content Distribution

2.1 Components of Future Internet Architecture

•name: It represents the interest expressed with the aid of the user specifying document name and format.

•content: it is the asked data.

•user: one who requests for content.

•producer: one who generates the content.

•Interest: it's a request for a particular report through the consumer. User requests for content the use of name.

•data Packet: It carries the content requested together with the name of that content.

•Node: A device in the network implementing NDN concepts.

•Interface: Connection of node to link.

•Router: In NDN functioning of routers is greater than routing a packet from consumer to producer. It has to preserve tune of incoming interests of consumers, data packet fetched to reply to the incoming interests and retaining the cache, ephemeral in-network storage.

•FIB: Forwarding Information base is maintained through every node in a network. It has data about path entries based on name prefixes.

•CS: content store is an ephemeral cache maintained at each node in a network. It's capable of storing recent responses (data packets) and interests. The scale of this storage could be different in different routers.

•PIT: Pending interest table. If the cache maintained does not have the data for the expressed interest, it stores the data name requested and the information about the interface in which the interest arrived.

2.2 Approach in NDN model

NDN is the future net architecture evolved to hold up with the ever growing amount of content being generated and disbursed over the internet. NDN is an example of content delivery network. It emphasizes on the data the consumer is interested in and now not where its miles stored. Data can be stored in which it became generated or within the cache of nearest node in a network. The bodily address of the nodes in which information is stored is not required in NDN not like TCP/IP. Since the bodily address is not essential for making verbal exchange feasible, there is no want of DNS to map names to IP addresses. On this architecture there are two sorts of packets: data packet and interest packet.

While the customer expresses his interest by means of specifying the name of the file i.e. Content name, this interest is forwarded in the network primarily based on the name of the content. Every intermediate node in the network has 3 entities related to it as cited in advance. On receiving interest, node first plays the name-based research of the requested content within the content store. If this node has the name of the content requested, then it responds with the data packet right away. This in-network garage allows the node to satisfy the request loamed. If there are a couple of customers requesting for the same content (often whilst a video is going viral at the net, multiple requests for the same content are obtained by using the server which hosts that content) an intermediate node which has the copy responds. For this reason there is no need to send a couple of requests for the equal content along the not unusual channel up to the node which holds the content. By using heading off sending comparable requests upstream, bandwidth is minimized. This optimization of hyperlink will lessen downstream latency. But if content store does no longer have the copy of the asked content, then PIT is checked. If PIT already has access inquiring for the content then intermediate node data information about the interest arriving interface.

On every occasion a reaction is obtained, data packet is forwarded to all such asking for interfaces and corresponding entries are deleted from PIT. Current PIT access indicates that interest has already been forwarded upstream by an intermediate node. Therefore, reproduction interest is not forwarded. If PIT does not contain an entry for expressed interest then incoming interest interface along with the name of the content and outgoing interface wherein interest is forwarded are dated in PIT after which those pastimes are routed in a network based totally on name prefix without the understanding of supply or destination cope with.FIB table is similar to IP routing table. It has data approximately name prefixes and interfaces in which it could be forwarded. These interfaces lead to supply which has the favored data. A couple of interfaces can be present for single name prefix. As a result an interest is forwarded to all viable paths and data may be retrieved from multiple paths.

2.3 Components of Current Internet Architecture

Protocols involved in TCP/IP: TCP, IP, UDP, ICMP.

• **IP:** net Protocol (IP) provides essential data for routing of packets in a network. IP isn't always a reliable protocol. To offer reliability, it has to group up with TCP. IP performs fragmentation, only if a network has described restrictions on the size of datagram.

•**TCP:** Transmission control Protocol (TCP) is Connection orientated protocol. It ensures the delivery of the TCP packets, making it a dependable technique.TCP protocol is carried out in process-to-process communications.TCP packets are encapsulated with extra data about addresses and IP datagram is built.TCP participates in a 3-manner Handshaking procedure. Which will make certain transport of Datagram it continues tune of sequencing and acknowledgments.

•**UDP:** user Datagram Protocol (UDP) is connectionless transport protocol. It does no longer guarantee delivery of packets. UDP is an unreliable method. For that reason it's far used in applications which includes video streaming in which failing to supply a single packet will not have an effect on the application. It does not carry out three-manner handshaking technique which ends up in less overhead. It does not maintain song of Sequencing and acknowledgments.

•**ICMP:** net control Message Protocol (ICMP) is applied to send manages messages between devices in a network. Control messages along with Host not accessible, Port now not accessible, Redirect messages to control traffic, source Quench message to control incoming traffic, message to notify expiry of Time to stay and so forth.

Other additives encompass:

•**IP routers:** they have only one dataarchitecture i.e. FIB.

•**IP FIB:** forward information base is beneficial to take switching decisions based on an IP address prefix fit. It consists of the information approximately the single outgoing interface i.e. Subsequent hop data most effective.

•**Buffer memory of IP**: as soon as packet is forwarded, it’s flushed out of buffer memory using MRU technique.

2.4 Approaches in TCP/IP Model

The 4 layer TCP/IP version has IP: internet Protocol located in its network layer. It offers with packaging data into datagram a good way to tour independently in a network. IP does now not keep a track of such datagram. Addressing and routing of those datagram is done inside the network layer of TCP/IP. With the expertise of the destination IP address, those datagram take distinct routes to attain the destination. Datagram reached at destination may be out-of-order or duplicated. IP is connectionless and unreliable protocol.

For reliability IP is paired with reliable protocols which include TCP. Transmission manipulate Protocol from the transport layer of TCP/IP model appears after the sequencing of all such datagram. TCP protocol establishes one-to-one connection, imparting reliable service. It sends the acknowledgement upon receiving the datagram so misplaced datagram may be detected and dispatched again. Traffic is managed by means of TCP. The utility layer of TCP/IP supports higher protocols along with DNS which maps the name to its physical address. As without physical address the connection cannot be established in TCP/IP.DNS makes use of TCP for important and bulk queries .IP handles the datagram routing primarily based on this physical address and datagram routing. While TCP might be accountable for better features such as offering reliability and error detection. This aggregate have become referred to as TCP/IP.

2.5 NDN Packet Format

In TCP/IP point to point path is installed based on knowledge of source and destination addresses. Path connecting the 2 points is the path alongside which packets are added. However in NDN technique any intermediate node which has the copy of requested content can reply. (It emphasizes on the „What‟ data the consumer is inquisitive about and no longer „in which‟ it is stored.) Therefore in NDN, concept of point to point information transport does no longer exist as those end points involved inside the connection can't be decided ahead.

NDN packets do no longer have fixed length headers. It enables to limit processing cost of packets. As a consequence packets of very small size may be transferred without the overhead. It gives the packets, flexibility. As opposed to fixed length headers the layout uses the TLV format to offer the flexibility of adding new types. This selection is capable of dealing with the state of affairs in the future wherein older types may additionally get discontinued because the protocol evolves over the time. This is a delivered advantage over TCP/IP.TLV stands for type length value. Primarily based on field data packets and interest packets are distinguished.

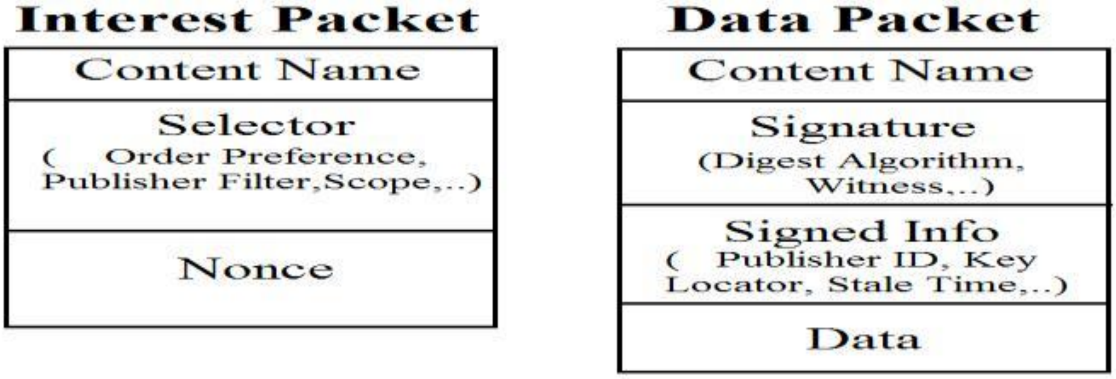

Fig 1: NDN Packets

Interest packets are composed of vital components that are content name and Nonce. Content name has precise name of requested data. Interest packets are uniquely diagnosed by way of the aggregate of name and Nonce. Nonce is generated at random via the client. It is used to differentiate among two one-of-a-kind consumers asking for the same content. At times it is able to show up that consumer is sending his interest again and again. This may additionally be diagnosed with the help of Nonce. Re-issuing the interest by means of customer indicates that the interest has not replied yet. Thus subsequent time router gets identical interest from same user; router forwards these hobbies on special interfaces. Nonce additionally enables to perceive an interest in advance forwarded which has looped back. For that reason looping interests are destroyed.

Similarly to these vital fields there exist a couple of optionally available fields including Selectors, scope, Interest lifetime which outline the behavior of interest packets. As a time selector subject is used for discovering and choosing the data that suits high-quality to expressed interest. The scope field defines how far interest packet can travel. The combination of name and Nonce need to uniquely pick out an interest packet. That is used to detect looping.

Data packet includes content name, met info, content (data), Signature.

Content name: NDN content has a hierarchical name including a chain of name components. Naming conventions in NDN are accompanied in a manner that only globally used entities are required to have globally precise names. Otherwise loamed identifiable entities could have local names for local context. A two level nested TLV is used to symbolize a name. Name is first detail and signature is final element of information Packet.

Met info field includes extra data about content kind, freshness period, finalblock id etc. Content kind can be set to default (=zero), hyperlink (=1), and KEY (=2). The default type indicates that real data bits are diagnosed by using name of data. The following kind of content link relates to some other name which is also used to identify real data content. The subsequent type of content, key is a public key. Freshness length is denoted by way of nonnegative range. It is an optionally available area. It is useful for substitute in content store if storage runs out of memory space. If freshness length is expired then corresponding data is marked as stale. Stale data is likewise a valid form of data. The expiration of freshness period takes into attention a possibility of era of newer model of the equal data. The finalblock id is an optional discipline which offers data about the final block within the series of fragments.

Data: The data packet represents some arbitrary binary information (held inside the content detail) together with its name.

Signature: With the help of Signature, generated content is connected to producer of that content. Signature presents more information about the writer. If the supply producer can be validated and relied on, each data packet signed via that producer also can be relied on. Therefore whilst data packets are retrieved from nearest router cache, they can be depended on based on their signatures. Therefore rather than securing the connection among supply and destination NDN attempts to relaxed each character data Packet by signing it. Signature in NDN is described as successive TLV blocks which might be signature info and signature value. Signature info tells extra about the description of signature, data that would be used to collect figure certificates. Signature information is protected in signature calculation. Signature value is not included in signature calculation. It represents real bits of the signature.

2.6 TCP/IP Packet Format

TCP is one of the widely used protocols in current net architecture. It moves the data in a continuous byte circulate that is suitable for bulk data transfer over the network. Full Duplex and reliable provider is likewise useful for interactive data applications. IP header presents all of the data that is useful for routing. It resources supply and destination IP Addresses, Time to live so that the undeliverable datagram are destroyed, sort of carrier to be provided which is used to determine managing of the datagram primarily based on elements like precedence, delay at some point of delivery.

IP headers additionally encompass area including Protocol which suggests which other protocol IP is paired with. It is used to suggest TCP, UDP or ICMP protocol this is utilized in delivery of Datagram. As stated earlier IP performs fragmentation if there may be a limit on size of datagram. In such conditions fields like Offset and Total length is useful.

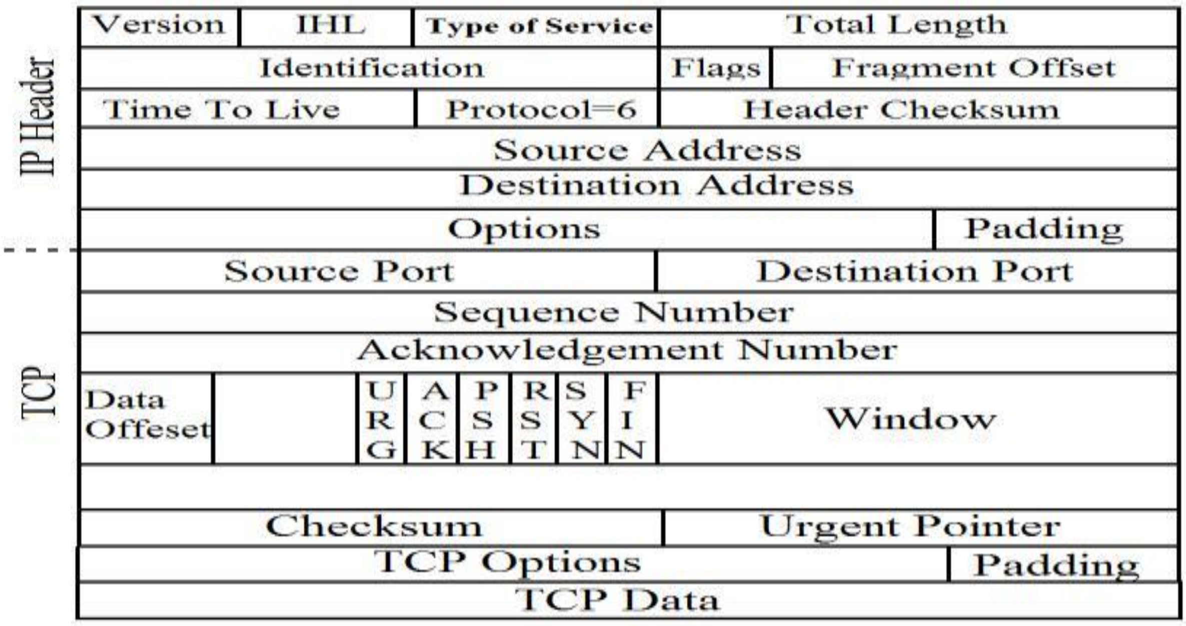

Fig 2: TCP/IP Packet

As stated earlier TCP provides a reliable connection using Three-way handshake also with the help of sequence numbers and acknowledgements. Thus there exists number of fields that support various services such as sequencing, acknowledgement of delivered packet, establishment of end to end channel etc. TCP is process to process communication protocol. Thus Ports help to identify processes that will communicate with each other. **Sequence Number** will help to packets to be delivered in sequence and **Acknowledgement Number** will ensure they have reached destination. **RST** and **FIN** used for tear down process. Checksum field is useful for error checking.TCP packets are encapsulated with IP datagram as shown in the diagram.

2.7 Security in NDN

One of the important aspects where modern-day and future net architecture differs is the safety. In NDN dynamic content Cache having a replica of asked content responds to the interest. Supply of content received can be different from where it becomes to begin with produced. For that reason it is very important to offer security to content. Attempt is made to comfortable the content itself as opposed to securing the connection via which content travels. Security NDN is content centric. The content can be secured from unintentional target market by means of imposing encryption mechanism. Encryption will assist to maintain confidentiality. Encrypted data may be decrypted with valid keys. Without those keys no intermediate node can benefit get access to data. Accordingly get right of entry to data is controlled. Safety of content has the following properties:

Provenance: It will determine origin or source of data.

Validity: this property will address concerns such as whether the received copy corrupted? Is the copy received complete? Etc.

Relevance: It will determine if data is relevant to interest expressed.

The relevance of the name of the content and content itself is essential. The consumer should get the content that they have requested. Thus there is the mechanism of keys which bind the content to its name by signing it. Sometimes this signature includes information about content producer. This additional information is in the form of key locator. It helps to determine provenance i.e. Origin of the data. It provides trust in data. User can rely on the signed data received. Integrity of data can be trusted if content is signed. Therefore, it is said that this signature securely binds together the tuple –
< Name, Content, Publisher's Key > – authenticating that the data is what its name purports it to be. Verifying signature in pieces of content can be time consuming. Thus verification of all content objects is expensive.

2.8 Security in TCP/IP

When evolution of the internet began, the principle motive became to connect two heterogeneous networks. Safety becomes no means of difficulty because the variety of customers becomes constrained. These days purpose of supplying safety over the internet is of high importance. These days' net customers are exposed to multiple protection threats. To tackle with them following mechanisms are carried out.

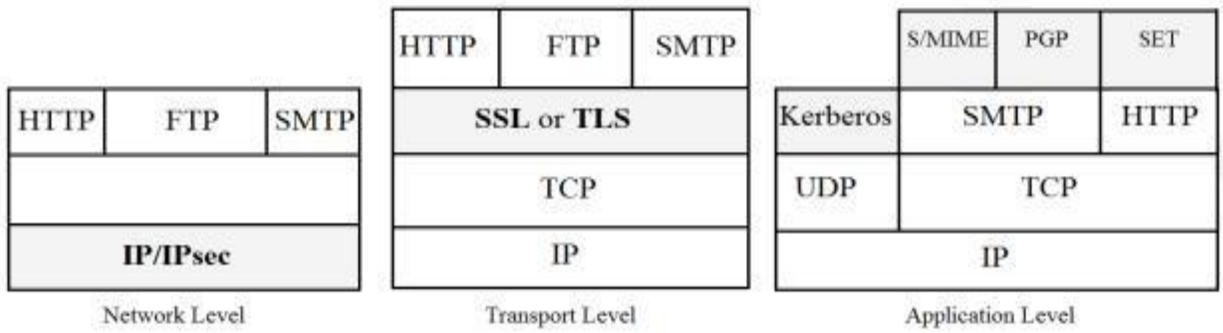

Fig 3: TCP/IP packet

IPSec IPsecurity is the suite of protocols providing security at the network layer. This is applied between host-to-host, network-to-network or host-to network to enhance security. With the help of security protocols such as Authentication Header and Encapsulating Security Payload it offers stronger authentication and encryption techniques. IPSec operates in two modes transport and tunnel mode. Transport mode focuses on an end to end security by protecting payload. Tunneling mode focuses on VPN by providing protection to payload, header and routing information.

AH protocol furnishes authentication, data integrity and protects against relay attacks. But it does not provide Confidentiality. In addition to what AH offers, ESP provides confidentiality. It uses various cryptographic techniques to achieve data integrity and authentication. Security Association (SA) is integral component of IPSec architecture. Security Association contains data needed for IPSec to function. It includes IP address of source, authentication keys, encryption key, key lifetime etc. Security association is unidirectional i.e. Two separate associations are required for inbound and outbound packet transfer. Key management is done by protocols like Internet Key Exchange. IPSec was designed for ipv6 but can be used for systems using ipv4.

HTTPS Hyper text transfer Protocol is an application layer protocol which works with Secure Socket Layer protocol of transport layer. This internet security standard was subsequently knows as Transport Layer Security (TLS). Whenever HTTPS Protocol is applied a secured connection is formed which is noticeable from the URL „https://‟. Such secured connections are useful for bank transaction or where data protection is priority. HTTPS encrypts data flow in

communication between client and web server. It uses public key encryption to secure the path which guarantees message integrity. When user wants to initiate a data sensitive operation, it sends a request to web server.
Web server invokes SSL Client and web server agree upon certain security parameters by participating in handshaking process. Web server then authenticates client by sending certificate and if the client trusts server that process continues. The communication path is secured using a symmetric key which is generated by encrypting session key with public key of server. Session key is generated on client side [10]. This Protocol protects data in transition by securing path only. But once data reaches destination responsibility to protect data depends on other processes. S-HTTP is another protocol used for encrypting web communication. It is used when part of data needs to be encrypted and HTTPS is used when most of the information is to be securely transmitted. In such cases HTTPS encrypts the entire communication channel. HTTPS is widely deployed to provide security over internet.

SET Secure Electronic Transaction was developed for conducting card transactions for VISA, MasterCard in a safe and secured environment. It includes authentication of customer and merchant. Transactions are carried out without revealing card details. This is possible because of Dual Signature. Dual Signature has information about order information for merchant and payment information for banks etc. in SET confidentiality is provided using encryption based on DES. SET ensures integrity of data transferred by using RSA signatures and SHA-1 hash codes. X.509v3 digital certificates are used for authentication in SET. Privacy of participants is maintained. It does not disrupt the functioning of other security protocols such as IPSec, SSL etc.

3.CONCLUSION

The concept in the back of this paper changed into to give the comparison of two internet architectures. On this paper differences in current and future net architecture are given which will help the reader to study ideas of new architecture with the aid of evaluating it with contemporary architecture. This evaluation will assist the reader to recognize the future internet architecture correctly. Future internet architecture is developed by using doing away with flaws of modern-day net architecture. Consequently to have a look at the future architectureit is encouraged to realize the fundamentals of present architecture supplied in this paper. These records will be beneficial for novices studying exclusive architectures of internet.

4. REFERENCES

[1] http://www.forbes.com/sites/jaymcgregor/2014/06/17/game-of-thrones-season-finale-becomes-most-pirated-show-in-history/s.

[2] Van Jacobson, Diana K. Smetters, James D. Thornton, Michael F. Plass, Nicholas H. Briggs, Rebecca L. Braynard , ‘Networking Named Content‟ (Palo Alto Research Center, Palo Alto, CA, USA)

[3] MishariAlmishari, Paolo Gastiz, Naveen Nathan, Gene Tsudik, „Optimizing Bi-Directional Low-Latency Communication in Named Data Networking‟.

[4] TCP/IP Protocol Suite fourth edition by Behrouz A. Forouzan.

[5] “NDN specification Documentation, Release 0.1a2, NDN Project Team, March 27, 2014.”

[6] http://named-data.net/wp-content/uploads/ndn_packet.png.

[7] http://www.cisco.com/web/about/ac123/ac147/ac174/ac196/about_cisco_ipj_archive_article09186a00800c8417.html

[8] Diana Smetters and Van Jacobson, Palo Alto Research Center, “Securing Network Content”.

[9] Katie Shilton, University of Maryland, College Park. Jeff Burke University of California, Los Angeles. Kcclaffy CAIDA/UC, San Diego .Charles Duan University of Colorado Law School .Lixia Zhang, University of California, Los Angeles, “A World on NDN:Affordances& Implications of the Named Data Networking Future Internet Architecture”

[10]ALL IN ONE – CISSP, EXAM GUIDE‟ fourth edition by Shon Harris. (CISSP, MCSE).