Nova Genesis - An Advanced Architecture for Internet of Things

Ajumol P A, Elizabeth Isaac

Abstract*: The Internet has become the most important medium for information exchange and the core communication environment for business relations as well as for social interactions. The current internet architecture itself might become the limiting factor of Internet growth and deployment of new applications including 5G and future internet. Architectural limitations of internet include weak security, lack of efficient storage and caching, data distribution and traceability issues, lack of interoperability and so on. The proposed system overcomes these limitations by an alternate architecture for internet called NovaGenesis. This architecture integrates the concepts of Information Centric Networking (ICN), Service Oriented Architecture (SOA), network caching and name based routing. ICN evolve internet from a host-centric model to a content-centric model through efficient data exchange, storage and processing. SOA enables software-control/management of network devices based on service requirements. Network caching improves performance in terms of throughput, network traffic and retrieval delay. Name based routing is for discovering and delivering of data. The framework proposed increases the scalability and reliability of the delivery of IoT data for services.

***Keywords* : Content Centric Networking, Cryptographic Hash Algorithm, Future Internet, Information Centric Networking, Internet of Things, ,**

I. INTRODUCTION

Internet is the new discovery by man that has revolutionized his working and living style. This has eliminated isolation entirely, breached all man-built barriers and built our planet a tiny area. On pressing a mouse, it took data to our doorway. Open what is called the 'Data Superhighway' before us. The internet is an vast knowledge network, where we use machines to interact with people over long distances. The internet helps us to use machines to collect knowledge from diverse sources and communicate with others. But Internet's function has changed drastically from its original intent, since it is free and open. To expand its reach, several evolutionary extensions have been added, such as IPSec, MobileIP, IPV6, and so on[1][2]. The best way to achieve this is with a Virtual Private Network (VPN) tunnel by encrypting data, if two or more places decide to exchange information anonymously, they need to conceal the information. IPSec is a rational consequence of encrypting data, because it enters an unsecured network such as the Internet. Similarly, mobileIP helps people to switch using the same Internet Protocol (IP) address from one network to another. It ensures contact continues without discontinuing users session or link. The IP address for finding the contact hosts on the network is used here. Many of these evolutionary extensions aim at satisfying the Internet of Things (IoT) dream[3]. IoT effectively links all of the smart devices (things) across the world utilizing sensors and actuators to communicate over the network.In this case, there would be a shortage of existing Internet advancements to completely endorse such multifaceted exponential innovations on the amount of com- puters, portability, interactivity, information, protection and privacy problems. Under the background of the Potential Internet (FI), only a few efforts have risen worldwide to reshape the Platform.The Internet of the future is a general concept for web study operations on modern architectures. Although the technological ad- vancement of the internet was from the outset an comprehensive study focus and raised popular knowledge of many crucial vulnerabilities in terms of functionality, efficiency, scalability, protection and several other categories including social, economic and business aspects lead to future internet research efforts [4]. Approaches to future internet vary from minor gradual innovative moves to full overhaul of clean- slate architecture concepts where the applicable technology is not constrained by existing standards or paradigms such as networking client-servers. IP address denotes both the identifiers as well as the locator of the end node, often referred to as textual overload as an illustration of a technical shortcoming of the internet protocol suite architecture solutions named clean slate are focused on knowl- edge that supplementary or late changes to the initial and existing specification are restricted to their adoption and introduction[5]. Technical examples of evolutionary strategies include additions to current Internet infrastructure, such as segregated facilities, efficient pooling of resources, separation protocol locator / identifier, and so on. NovaGenesis is an architecture hybrid name-centered, service-centered, information-centered, host-centered, software-defined, mobile-friendly, self-organizing[6]. It can be used as the Future Internet network. The goal is to create a clean slate platform for exchanging and exploring information of the future generation. It can be interpreted as a Future Internet initiative. It attempts to provide a practical context for convergent technology growth. It started in 2008 at Inatel, in Minas Gerais, Brazil. NovaGenesis adopts the idea of the Internet of Knowledge and Services (IoIS), in which content-centered and service-centered approaches are combined to integrate the processing, storing and exchange of information.

Revised Manuscript Received on April 21, 2020.

***** Correspondence Author

Ajumol P A, Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India, ajumolantony0203@gmail.com

Elizabeth Isaac, Assistant Professor, Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India, elizabeth.issaac@gmail.com

This Paper addresses the following strategies for modeling NovaGenesis architecture for IoT

- Efficient sharing, storing and retrieval of IoT data through a framework for information-centered networking (ICN).
- Dynamic structure of contract-based IoT services.
- Software-control / IoT system configuration according to operation specifications.
- Naming and name resolution of real and abstract entities, demonstrating the separation of identifiers / locators and the self-organization of the rich semantics.
- Name-based routing and network caching.

Authenticating the Internet-of-Things (IoT) devices in mobile systems is extremely challenging, because there will be billions of the IoT devices.SHA-256 Cryptographic hash function based authentication mechanism is used for software control management of IoT devices.

II. RELATED WORKS

The introduction of Future Internet Architecture (FIA) into the world's existing mobile network is still underway. A comprehensive FIA communications infrastructure also calls for a stable network to allow for greater scalability and efficient resistance to hazards. New analysis on the FIA security strategy shows that they are not cost-effective, so they use a complex encryption scheme that limits applicability to free, protected contact.

The Conventional Internet Architecture Paradigm faces a resource limitation that raises a question of real-time scalability as vast numbers of Internet of Things (IoT) nodes combine to achieve the same purpose. In addition to the scalability due to non-flexibility and loss of control structures, it also faces a non-synchronous degree of agility and high-dimensional transmission of knowledge in advanced communication networks[7]. The 32-bit IPV4 architecture promoting an extended 128-bit IPV6 solves the scalability problem, but the host-based IP network paradigm is not appropriate for modern and sophisticated web-based unified networking where widely dispersed and transparent internet access is required. Fourth-generation networking networks such as 4 G, 4G-LTE and 5 G are built to promote the distribution of high-dimensional internet connectivity that enables the next device to be a web-centric infras- tructure.Regardless of the various mitigation mechanisms introduced in the security aspect of IPV4 and IPV6, such as IPsec, DNSSec etc.[8], the tradition of safety vulnerabilities, and the vulnerability always exits.The coin side faces new challenges and risks as an unremitting rise in internet penetration is faced with dissemination and uploading among user bases where protection is a very important problem in the security policy domain[9].Consequently, the quality of the material of potential network design is an critical and daunt- ing topic that needs to be tackled.Because content delivery to the consumer involves a major change in the network infrastructure, new types of distribution models are evolving, but no particular version has been created, whereas various storage technologies such as SDN, cloud, virtualization, etc. are increasing, with several protection concerns, information management capabilities, interoperability, etc. The action of both the copyright owner and the web user is the same, so the copyright owner never permits an illegal or non- subscriber to access or display their products because the Internet service company is subjected to a substantial economic danger. The resolution process has observed third-party vendors handling data security paradigms as an extra cost business activity, as well as other cases in which the third party is found responsible for loss of protection[10]. Since the broad range of academics and researchers with an emerging and complicated internet technology environment require new solutions that are effective, reliable, and scalable to manage identity protection, continuous and substantive contributions are required to address this challenge. Although modern public- private key cryptography (PPKC) uses a variety of complicated and hard encryption methods with a secret key to have a higher degree of context security, it faces a huge overhead technical and time complexity that is not sufficient for the energy-efficient and cost constraints that will be applied in the future. To create control of access in the FIA system in elliptical curve cryptography [11]. The [12] study introduced a simulation of protection that used a software-defined network.[13] study introduced a method that can be used to assess the IoT associated protection intensity. .Ambrosin considers protection and confidence as impor- tant[14].Device stability[15], where the physical layer was used when [16] used the confidence dimension as part of the evaluation. Safety is also a problem in the FIA context, particularly when it addresses the large data scale and Cha et al's research[17] has given a conceptual answer to that. Safe sharing of data through software- defined networks has also been shown to be more efficient[19]. Work in [20] lso dealt with the use of digital technologies, along with the integration of knowledge. The research conducted in[21] constructs an entity's architecture utilizing an event-driven method to establish the coordination process over a large network. The largest of the new offensive against FIA is focused on internet-of-things-connected securities which are seen as having an effect on a broad network's security applications.

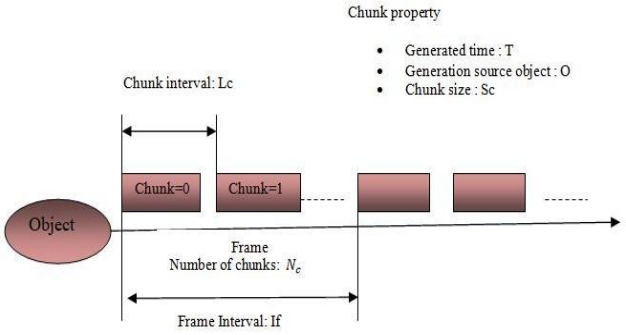

Fig. 1. Definition model for stream data

III. INFORMATION CENTRIC NETWORKS

The Internet was created about 50 years ago, when it concentrated largely on intercomputer machine contact. Therefore the internet net- work depends on peers at the networking platform [22] Through extending the World Wide Web (WWW), however, Internet consumers are interested mainly in details rather than terminal position, although access is still based on the site itself.

Future internet is supposed to be a post-IP network, where content- centric networking (CCN) or information-centric networking (ICN) as such is promising as a potential communications framework, solving the problems raised by such a distance. CCN has discussed a number of organizational initiatives. In this paper we concentrate on CCN- focused networking with IoT products.

CCN distributes knowledge through the Consumer Benefit Packets. If a client wants to view data, a Value packet can be forwarded by the user to networks comprising the term of operation. It may be distributed by object word by the router obtaining an attraction. A domain server accepting an Interest packet will forward it back to the customer as a data packet pointing to the Interest packet [23]. All routing is then accomplished by service-oriented, as CCN guarantees user-centric communication dependent on the domain name. The CCN architecture may be used to support various purposes, such as video sharing, M2 M networking, collection of sensor information, etc. The proposed framework constructs a mechanism for networking which facilitates communication with IoT devices. As proof of concept we show our implementation and experiment with a NovaGenesis host operating temperature sensor and a laptop.

Fig.1 demonstrates simulation of Stream results. Event generates the data frames sequentially over time [24]. Data frame is a storage package that is demanded from an Value packet. If the data frames are created as time interval, we identify frame interval. When a data frame demands a packet of interest, the data frame is broken into chunk of data.Data chunk is a data fragment separated according to the scale of the MTU (Maximum Transmitting Unit). The *Ic* chunk interval is known as the time interval at which chunks of data are being transmitted to the network. Frame interval and portion period may be unknown interest. Additionally, in one data frame we define the number of chunks as *Nc*. The block of data contains the details about the property which is the time produced, the entity that created the data and the size of the data.

Multiple tools, including the sensor network and the home net- work, perform the role in a organized way in M2 M area. In order to understand the communication, it is important to share details between devices and delegate the process to other devices. We describe object control as a request for the defined operations therefore for a given entity. Object has the details about the property which is the name of object N, and the set of possible acts A. Requester transfers object access *Ot* to the goal object and *Areq* to the test item. Control of the sent entity is forwarded to an item that satisfies N=*Ot*. Object that obtained object control executes the action demanded, and then returns the response as a message to the requester.

Stream data comprises a set of information, and stream data retrieval includes retrieving those pieces of info. There are usually two forms of removing a sequential material.

- Control messages as interest packets: When the client begins gathering information, it sends an interest packet demanding ”begin data recovery.” A sequence of contents is continuously performed by the server processing the Interest packet. If after- wards a customer decides to interrupt the operation, a Regular packet would be submitted asking for the data collection to be halted.
- Sending Interest packets to show details on their own: for each item, the user sends a Packet of Interest. The node obtaining the Meaning packet sends out the information at issue. The amount of Interest Packages would be the same as the number of ordered things. The first method would be to slice the packages [25]. Then, both the client and the server must do the session and retransmission of the data. Additionally, the architecture of CCNx does not support requesting multiple Data packets from a node. The second option won’t have to handle retransmission of sessions and material. The client sends more Value packets than before, but some stream data can be quickly retrieved by the client. We are therefore following the above method for the communication of stream data. Nonetheless, if we can make any improvements to the CCN nodes (end terminals and CCN routers), we can recall the previous process.

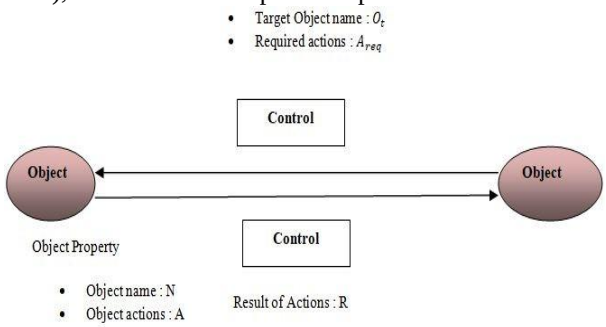

Fig. 2. Modeling of Object Control

1V. SYSTEM ARCHITECTURE

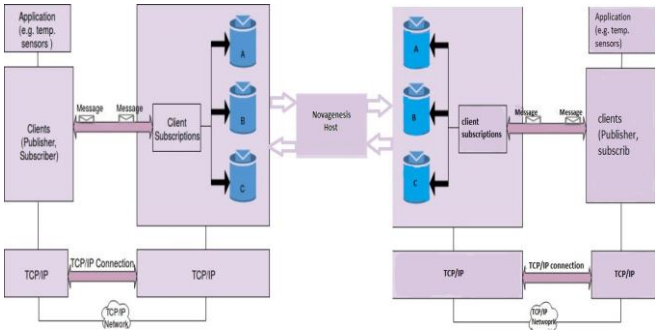

Fig.3.Proposed System Architecture

NovaGenesis Architecture (NG) is a collection of distributed systems built to build, store, and exchange converging knowledge. This also includes the open Internet, cloud infrastructure, service-oriented architecture (SOA), knowledge-centric networking (ICN), and IoT. That information processor in the design of NovaGenesis is used as a tool such as networking equipment, implementation of network protocols, on- line servers, peer-to-peer software, machine-to-machine systems etc. This relies on the software’s three components: I Name Resolution and Network Cache (NRNCS); (ii) Proxy / Gateway / Controller (PGCS) for message encapsulation over communication interface systems such as Ethernet, Wi-Fi and IEEE 802.15.4; and (iii) device implementations.

New technologies should change the traditional 'receiver embraces all' paradigm to a publish / subscribe paradigm. Providers post content in the pub / subframe, while other register. It has a distribuIt publishes and subscribes ted hash table (DHT) and name connections. If a name is provided that is binding on DHT a provider determines which other services to connect to this NB are needed. Instead, a dealer provides an request (or an NB), which requires entry to all facilities. Before it is transmitted, a telecom network target must be submitted to the data. It allows permitted knowledge and name relations to be distributed. A proxy is an aspect that represents the allocation of other organizations' diverse capital. In the case of IoT, a proxy may be used as a "smart agent" disclosing the capabilities of the device(s) and the available tools for creating SLA to interested providers. A gateway is a connection between various technologies, or the place of entry / exit. An IoT gateway is liable for removing raw data across the Internet; in some situations it performs data interpretation and semantine annotation. Finally, a controller is a system that controls or performs decisions with respect to systems of physical resources or other resources. Throughout the sense of IoT, the theory of NovaGenesis seeks to implement SDN concepts more broadly, i.e. to use device controls to customize functionalities rather than to forward frames. Fig.3 depicts the data flow between each participating node. There are two nodes which is two ESP-8266 controllers that will send and recieve data through the host. The host is connected with the two nodes via internet. On transmitting the message from one node to the another it will pass the device id,message,etc. The host will acknowledge or not acknowledge for the success and failure. The data is routed to the other node by the host computer which will forward the data.

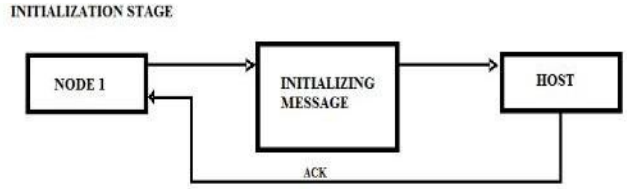

Fig. 4. Initialization

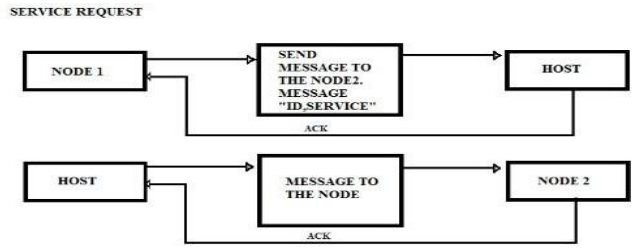

Fig. 5. Service Requesting

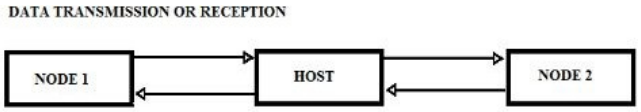

Fig. 6. Data Transmission

The requesting of service is also done using messages by the node to the host. Selecting the more priority node are also the role of the host. The host will generate a log which will inform about the connection established, data transmission, connection termination. The host will be tracking th process in the nodes also via log.

A. SHA-256 Cryptographic Hash Algorithm

NRNCS is introduced using cryptographic hash function SHA-256 and Message Queuing Telemetry Transport (MQTT). SHA- 256 (Secure hash algorithm, FIPS 182-2) is a 256-bit digest-length cryptographic hash feature. It's a keyless hash feature, that is, an MDC (code for manipulation detection). A message is processed by blocks of 512= 16 * 32 bits, each block requiring 64 rounds.

1) Basic operations:

AND, XOR and OR processes, denoted by , *and* , respectively. Bitwise add-on, denoted by ¯. Number Modulo 232, denoted as A + B

We each run on 32-bit characters. Binary terms are represented as integers written in base 2, for the last operation.

- RotR(A, n) denotes the circular right move of the binary term A by n bits.
- ShR(A, n) denotes the right move of the binary term A by n bits.
- A||B denotes the concatenation of the binary words A and B.

2) Functions and constants: The algorithm uses the functions:

$$Ch(X, Y, Z) = (X \wedge Y) \oplus (X \wedge Z) \quad (1)$$

$$Maj(X, Y, Z) = (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z) \quad (2)$$

$$\Sigma(X) = RotR(X, 2) \oplus (X, 13) \oplus RotR(X, 22) \quad (3)$$

$$\Sigma(X) = RotR(X, 6) \oplus (X, 11) \oplus RotR(X, 25) \quad (4)$$

$$\sigma 0(X) = RotR(X, 7) \oplus (X, 18) \oplus RotR(X, 3) \quad (5)$$

$$\sigma 1(X) = RotR(X, 17) \oplus (X, 19) \oplus RotR(X, 10) \quad (6)$$

and The 64 binary terms Ki supplied in the first 64 prime numbers by the 32 first bits of the fractional portions of the cube roots:

0x428a2f98	0x71374491	0xb5c0fbcf	0xe9b5dba5	0x3956c25b	0x59f111f1	0x923f82a4	0xab1c5ed5
0xd807aa98	0x12835b01	0x243185be	0x550c7dc3	0x72be5d74	0x80deb1fe	0x9bdc06a7	0xc19bf174
0xe49b69c1	0xefbe4786	0x0fc19dc6	0x240ca1cc	0x2de92c6f	0x4a7484aa	0x5cb0a9dc	0x76f988da
0x983e5152	0xa831c66d	0xb00327c8	0xbf597fc7	0xc6e00bf3	0xd5a79147	0x06ca6351	0x14292967
0x27b70a85	0x2e1b2138	0x4d2c6dfc	0x53380d13	0x650a7354	0x766a0abb	0x81c2c92e	0x92722c85
0xa2bfe8a1	0xa81a664b	0xc24b8b70	0xc76c51a3	0xd192e819	0xd6990624	0xf40e3585	0x106aa070
0x19a4c116	0x1e376c08	0x2748774c	0x34b0bcb5	0x391c0cb3	0x4ed8aa4a	0x5b9cca4f	0x682e6ff3
0x748f82ee	0x78a5636f	0x84c87814	0x8cc70208	0x90befffa	0xa4506ceb	0xbef9a3f7	0xc67178f2

3) Padding: **To ensure that the message1 has length multiple of 512 bits:**

- a bit 1 is appended first
- Next, k bits 0 are introduced, with k being the smallest positive integer, so that l + 1 + k = 448 mod 512, where l is the bits duration of the original message , the length l of the original communication is appropriately 64 bits and these bits are inserted at the end of the response

The message is still to be extended, particularly though the original duration is only a 512 multiple.

*4) **Parsing the Message:*** The message and its padding will be interpreted in N m-bit bytes. Because the input block's 1024 bits can be represented as sixteen 64-bit words. We use the original hash values and 64 constants to work out the 32 byte digest code.

use MQTT broker software to build a publish / subscribe program. There are two categories of network entities specified in the MQTT protocol: a message broker and multiple clients. An MQTT broker is a server that accepts all messages from the clients and then routes the messages to the appropriate clients for the target. An MQTT client is any system that runs a MQTT library and connects to a MQTT broker over a network (from a micro controller up to a complete server).

V. RESULT AND ANALYSIS

We report results for scenarios with physical and virtual hosts. First we have implemented a scenario with a MQTT box and Host that runs NovaGenesis software. MQTT box is implemented as Pub/Sub model which will publish and subscribe the data that are transmitted through the network Fig 7 depicts the creation of client component for communication. Client publishes the data via MQTT protocol; NovaGenesis module running on the host will receive the data published by the client. For that we have to initialize all the communicating nodes to this NovaGenesis network. Using SHA-256 Cryptographic Hash function a 32 byte unique identifier (name binding) is created for each nodes.All the name bindings are recorded on log file (Hash Table). Fig.8 illustrate the graph connecting all the nodes in the network. Each nodes are identified with their 32 byte unique id. On successful creation of nodes,we can start communication.Client sends the data to host by publishing it to the network. Host will receive the data along with the data rate of network. Secondly, we have implemented a scenario with two wifi module based controllers. These two nodes are connected to the NovaGenesis host via internet.The two controllers used here is ESP2866 nodeMCU. The nodes are sending preset data over the network. Embedded NovaGenesis has smaller specifications for RAM and ROM compared with equivalent RPL + 6LowPAN stacks. In a local area network, data sharing was done in a few milliseconds.

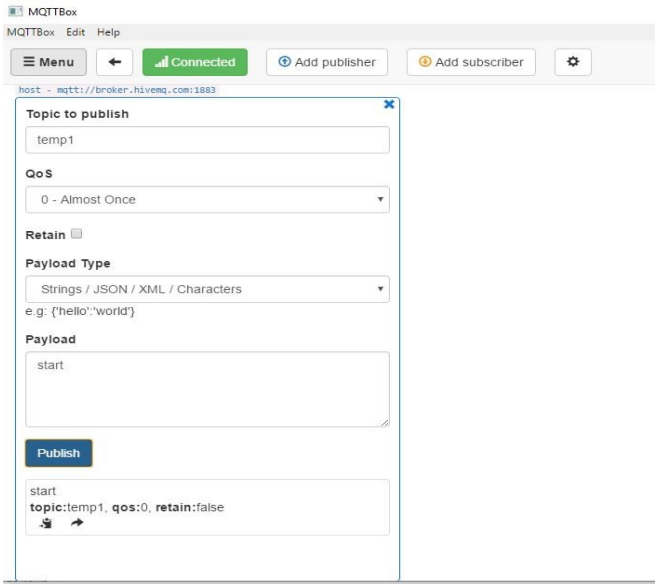

Fig. 7. Creating Client Component

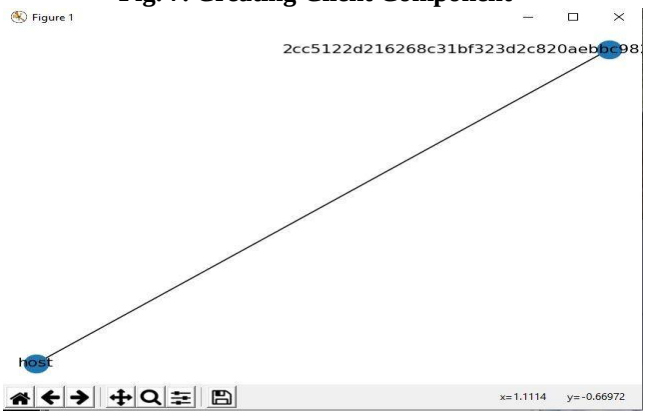

Fig. 8. Graph Connecting nodes with 32 byte Unique Identifier

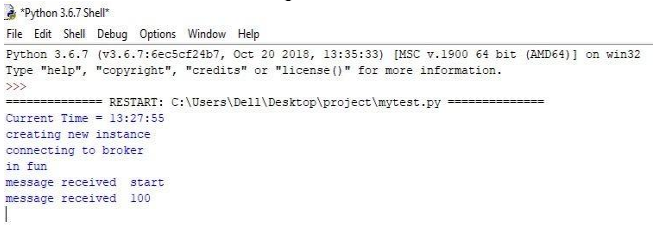

Fig. 9. Reception of Data

VI. CONCLUSION

NovaGenesis usually integrates FI/5 G / IoT structure paradigms that are implemented separately. Information-centric networking (ICN) has been developed to store, preserve and distribute raw data via the scalability and durability of IoT data delivery for services. Integrating IoT structures and their life cycles, service-oriented "semantic matrix" and context-based orchestration design. ICN and SOA were introduced to promote the identification and acquisition of services by utilizing name-based routing and naming the specified entities.

Self-verifying marks for provenance of IoT origins and accuracy of data were introduced. Infinite namespaces have been developed that include common vocabulary (e.g., keywords) and self-verifying names (e.g. hash codes) with all architectural orga- nizations. It also displayed Integrated Name Resolution for artifacts, gateways, users, vendors, and information.In addition to state-of-the- art operational arrangements, NG has authorized programming of the IoT devices accordingly. In other terms, services report roles to other devices, enabling service-defined adjustment of computer parameters and functionalities – a revolutionary idea called service- defined architecture.

REFERENCES

1. A. M. Alberti, "A conceptual-driven survey on future internet require-ments, technologies, and challenges," Journal of the Brazilian Computer Society, vol. 19, no. 3, pp. 291–311, 2013.
2. C. Partridge, "Helping a future internet architecture mature," SIGCOMM Comput. Commun. Rev., vol. 44, no. 1, pp. 50–52, Dec. 2013.
3. J. Li, Y. Shvartzshnaider, J. A. Francisco, R. P. Martin, K. Nagaraja, and D. Raychaudhuri, "Delivering internet-of-things services in mobilityfirst future internet architecture," in 2012 3rd IEEE International Conference on the Internet of Things, Oct 2012, pp. 31–38.
4. S. Vrijders, D. Staessens, D. Colle, F. Salvestrini, E. Grasa, M. Tarzan, and L. Bergesio, "Prototyping the recursive internet architecture: the irati project approach," IEEE Net., vol. 28, no. 2, pp. 20–25, March 2014.
5. A. M. Alberti, M. A. F. Casaroli, D. Singh, and R. da Rosa Righi, "Naming and name resolution in the future internet: Introducing the novagenesis approach," Future Generation Computer Systems, vol. 67, pp. 163 – 179, 2017.
6. C. Dannewitz, D. Kutscher, B. Ohlman, S. Farrell, B. Ahlgren, and H. Karl, "Network of information (netinf) - an information-centric networking architecture," Comput. Commun., vol. 36, no. 7, pp. 721–735, Apr. 2013.
7. 1. Huang, T., Yu, F.R., Xie, G., Liu, Y.: Future internet architecture and testbeds. China Commun. 14(10), iii–iv (2017)
8. Kent, S., Seo, K.: Security architecture for the internet protocol. Docu- ment RFC 4301 (2005)
9. Evans, D. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything;White Paper 2011; Cisco Internet Business Solutions Group (IBSG), Cisco Systems, Inc.: San Jose, CA, USA, 2011.
10. C. Dannewitz, D. Kutscher, B. Ohlman, S. Farrell, B. Ahlgren, and H. Karl, "Network of information (netinf) - an information-centric networking architecture," Comput. Commun., vol. 36, no. 7, pp. 721–735, Apr. 2013.
11. T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica. A Data-Oriented (and Beyond) Network Archi-tecture. In Proc. of SIGCOMM, August 2007.In: 2013 IFIP Networking Conference, Brooklyn, NY, pp. 1–9 (2013)
12. P. Martinez-Juliai and F. S. Antonio, "Empowering the internet of things with software defined networking," FP7 European research project on the future Internet of Things, .Intelligence and Security (CIS), Shenzhen, pp. 390–393 (2015)
13. S. Haller, S. Karnouskos, and C. Schroth, "The Internet of Things in an Enterprise Context," in Future Internet – FIS 2008 Lecture Notes in Computer Science Vol. 5468, 2009, pp 14-28.
14. Ambrosin, M., Compagno, A., Conti, M., Ghali, C., Tsudik, G.: Security and privacy analysis of national science foundation future internet architectures. IEEE Commun. Surv. Tutor. 20(2), 1418–1442 (2018)
15. Object Management Group, "The Real-Time Publish-Subscribe Wire Protocol DDS Interoperability Wire Protocol Specification", OMG, Version 2.2. Sep. 2014.
16. Sehgal A, Perelman V, Kuryla S, Schonwalder J. Management of resource constrained devices in the internet of things. IEEE Commu-nications Magazine. 2012 Dec;50(12).
17. Zhang, J., Zhang, X., Imran, M.A., Evans, B., Zhang, Y., Wang, W.: Energy efficient hybrid satellite terrestrial 5G networks with software defined features. J. Commun. Netw. 19(2), 147–161 (2017)
18. Simpson, S., Shirazi, S.N., Marnerides, A., Jouet, S., Pezaros, D., Hutchison, D.: An interdomain collaboration scheme to remedy DDoS attacks in computer networks. IEEE Trans. Netw. Serv. Manag. 15(3), 879–893 (2018)
19. N. Fotiou, P. Nikander, D. Trossen, and G. Polyzos, "Developing information networking further: From PSIRP to PURSUIT," in Broad-band Communications, Networks, and Systems (I. Tomkos, C. Bouras,
20. G. Ellinas, P. Demestichas, and P. Sinha, eds.), vol. 66 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 1–13, Springer Berlin Heidelberg, 2012.
21. B. Ahlgren, P. Aranda, P. Chemouil, S. Oueslati, L. Correia, H. Karl,
22. M. Sollner, and A.Welin, "Content, connectivity, and cloud: ingredients for the network of the future," IEEE Communications Magazine, vol. 49, pp. 62–70, July 2011.
23. Alberti, A.M.; Casaroli, M.A.F.; Singh, D.; da Rosa Righi, R. Naming and name resolution in the future internet: Introducing the NovaGenesis approach. Future Gener. Comput. Syst. 2017, 67, 163–179. [CrossRef]
24. T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim,
25. S. Shenker, and I. Stoica, "A data-oriented (and beyond) network architecture," ACM SIGCOMM Computer Communication Review, vol. 37, pp. 181–192, October 2007.
26. V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in Proceedings of 5th International Conference on Emerging Networking Experiments and Technologies, pp. 1–12, December 2009.
27. M. Mosko, I. Solis, and C. Wood, "CCNx Semantics," Internet- Draft draft-irtficnrg- ccnxsemantics-01, IETF Secretariat, January 2016. http://www.ietf.org/ internet-drafts/draft-irtf-icnrg-ccnxsemantics-01.txt.
28. D. Raychaudhuri, K. Nagaraja, and A. Venkataramani, "MobilityFirst: A robust and trustworthy mobility-centric architecture for the future internet," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 16, pp. 2–13, Decenber 2012.

AUTHORS PROFILE

Ajumol P A received Bachelor of Technology in Computer Science and Engineering from KMEA Engineering College, Edathala, Aluva in 2018 and currently pursuing Master of Technology in Computer Science and Engineering from Mar Athanasius College of Engineering, Kothamangalam affiliated to APJ Abdul Kalam Technological University. Her research interest is in Network Technology and Network Security

Elizabeth Isaac is currently working as assistant professor in the Department of Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India. She received her B.Tech degree in 2008 in Computer Science and engineering from Mahatma Gandhi University, Kottayam and M.Tech in 2010 in Computer Science and Engineering from Vellore Institute of Technology. She received her PhD in 2018 from Vellore Institute of Technology. She is interested in the area of Computer Architecture and Network on chip.