EAI Endorsed Transactions
on Energy Web
Research Article EAI.EU

Survey Based on Security Aware Caching Scheme for IoT Based Information Centric Networking

M. Sakthivanitha[1,*], S. Saradha[2]

[1]Research Scholar, Department of Computer Science,
VELS Institute of Science Technology & Advanced Studies (VISTAS), Pallavaram, Chennai, Tamilnadu, India.
[2]Assistant Professor/Research Supervisor, Department of Computer Science, VELS Institute of Science Technology & Advanced Studies (VISTAS), Pallavaram, Chennai, Tamilnadu, India., saradha.research@gmail.com

Abstract

Information-Centric Networking (ICN) empowered by information-centric paradigm takes popular paradigm place of host-centric networking of communication networks, which in turn helps prioritizing the labeled content delivery, with no information on the origin of the contents. Security of client and content, originating place, and identity privacy are inherent in ICN paradigm design in contrast to present host centric concept where they are introduced as a second-thought. But, with its genesis, the ICN paradigm exhibits different unresolved challenges in privacy and security. In this work, current literature in ICN privacy and security are explored and open challenges are presented. Especially, three extensive subjects: security threats, risks involved with privacy, access control management techniques are explored. Primary objective of ICN is to modify the present location-based IP network architecture to location-free and content-oriented network framework. ICN can satisfy the demands for caching to the neighbouring edge devices with no more storage deployed. In this work, an several architecture for effective caching at the edge devices for data-centric IoT applications and a rapid content access that depends on novel deep learning techniques and caching processes in ICN. The novel learning-oriented effective caching technique yields the solution to the problem involving the available hash and on-path caching techniques, and the newly introduced content popularity scheme improves the availability content at the devices in the vicinity for minimizing the content transfer time and packet loss ratio.

Keywords: Information-Centric Networking (ICN), Caching Scheme, Deep Learning Approaches, VANETs, MANETs.

Received on 16 May 2020, accepted on 15 July 2020, published on 04 August 2020

doi: 10.4108/eai.1-7-2020.165960

*Corresponding author. Email:sakthivanithamsc@gmail.com

1. Introduction

Each and every device is connected to internet via IoT. It allows accessing of those devices by any path at any location at any time, for example from any network [1]. Enchanted objects like smart vehicles, smart meters, smart-phones, smart microwave ovens, smart refrigerators and smart washing machines are included in IoT. Various remarkable as well as valuable applications like smart cities, smart gird, digital health, smart transport, smart building, and smart home are enabled because of these smart objects connectivity. Huge amount of data will be generated, if billions of these smart devices are connected to internet as a consequence. Data produced in YouTube videos, Facebook needs to combine with this IoT data in IoT big data. Hence, effective access and search of IoT Big Data has imposed multiple limitations on the background TCP/IP architecture when bringing several significant challenges.

Among these challenges, one involves naming space being i9depleted, and in future, IPv6 address space may also be depleted. Also, IPv6 address is extremely long and its longer length rendering it less (and addressing) all the IoT devices [2]-[3]. IPv4 addressing is appropriate for communication using constraint-based devices such as wireless sensors [4]-[5]-[6]. Hence, effective naming and addressing approaches for several billions of devices (also contents) are not truly accessible in IP-architecture. In addition, each device is imposed with multiple limitations and specifications that introduce another problem of heterogeneity. This states that IoTs reside on heterogeneous devices with respect to expense, battery life, memory, size and processing power. Apart from this, various devices are constraint based, inexpensive, memory restricted, low power and small wireless sensors and they are generally termed as smart devices.

Along with heterogeneity, insufficient memory as well as inadequate battery life constraint-limited devices, there is frequent data unavailability can become which in turn, leads to data being unavailable. Hence, the solutions such as in-network caching (which are necessary for enabling the data availability) are not present in the ordinary IP-based networking. Also, applications of IoT like smart health, smart grid and smart home requires more privacy and security with respect to device accessing data and utilization of those data [7]. Better management of mobility is needed in few applications of IoT like smart transport, MANETs, and VANETs [8-9].

Then again, in data point of view, users of several IoTs application show more interest in being provided with updated information instead of just knowledge on information source's address. To give an example, IoT devices particularly in domain known as wireless sensor networks (WSN), work towards the particular goal of information extraction on a massive scale basis [10]. Each device is required to carry out some a certain task, for instance, temperature sensors perform the temperature measurement in their environment and has no relevance of performing task of word processing usually done using general purpose computer. Anyone using applications of temperature measurement is concerned about particular region's current temperature value instead of temperature value from a certain sensor.

When the conventionally designed TCP/IP in the form of network architecture for IoTs is considered for connecting very a smaller number of computers and sharing less and in-economic network resources using the restricted address space at the network layer, it is surely not developed for meeting the demands of IoTs. Also, in addition to the above-stated needs, the massive data has imposed surplus requirements like data distribution and scalability on the background framework. In order to satisfy these IoTs requirement, Information-Centric Networking (ICN) is presently evolved as a suitable solution. Until now, nine important frameworks introduced under ICN concepts includes, Green ICN, C-DAX, Mobility first, CONET, CURLING, NetInf, PURUSUIT, CCN and inclusive of DONA, [11-18]. In these ICN-based frameworks like CNN, CONVERGENCE, COMET, SAIL and DONA are dirty-slate, NDN, PURSUIT and MF are clean-slate frameworks. CCN (NDN) is a popular technique in ICN-based novel architectural frameworks [19]. The major features of ICN consist of in-network caching, contents naming, remarkable and flexible management of mobility, scalable information delivery and enhanced security that are generally ideal inIoT applications. Also, hourglass architecture based on ICN yields a thin-waist like TCP/IP [20]. Besides this, ICN can cloak over TCP/IP network or MAC layer. CCN is used just over MAC layer of WSN. The present literature [21]-[22] debates that ICN tries to replace IP; instead it is believed and forecasted that ICN is an overlay network on IP network top. Truly, CCN layer, which cloaks content association necessity with IP address rather than name. Real content delivery is required in TCP/IP interface or direct MAC (layer 2) interface.

One remarkable advantage of ICN is, in-network caching, can effectively deal with information delivery problem from inactive (inaccessible) device owing critical life of battery through contents caching at intermediate nodes. In addition, it reduces their trivial delay in active devices using caching. In addition, naming the contents is used to resolve address space scarcity problem of IPv4 and can facilitate scalability effectively and can also carry out name management effectively and help in easily retrieving the massive data generated by IoT applications. In addition, mobility management yields good hand-off of mobile devices like vehicles and mobile phones. Self-certifying contents of ICN yields much better security to data instead of just protecting the hosts [23]-[21]. Hence, the above constitute the reasons that in this work, naming based on ICN, in, mobility and security, network caching approaches are surveyed and examined in IoTs.

In this work, Section I analyses the about the connection between the IOT and its applications. Section II the features of IOT are discussed to analyse its security features, Section III clearly discuss the working procedure of ICN in detail, Section IV discuss the need of ICN for IOT applications, Section V provides the overview on the classical approaches that are employed for security aware IOT and ICN networks ,Section VI provides the comparison of the research strategies along with its benefits and drawbacks, Section VII discuss the solution to enhance the security aware cache framework ,Section VIII discusses the results of simulation. The conclusion and work intended for the future are discussed in Section X.

2. Internet of Things (IoT)

Fundamental concept of Internet of Things (IoT) [18] is connecting every object with Internet for facilitating intelligence characteristic of those objects. Therefore, different methods are integrated, to allow actuators and sensors for perceiving and gathering required data, for interaction and coordination to get smart data analytics as well as making human involvement free decisions. Fig.1illustrates important benefits of IoT.

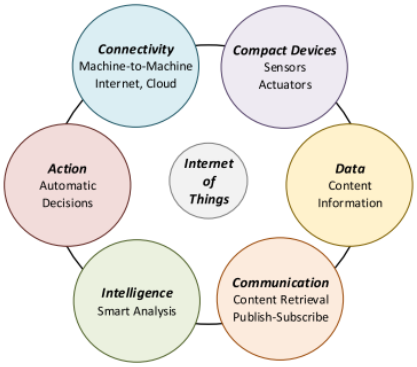

Figure 1. IoT Features & Advantages

IoT is a sophisticated network, which indicates the convergence of several realistic fields, where every domain exhibits its individual features. The important features are listed below:

Sensing: This characteristic utilized in large amount of IoT use cases, like: climatic monitoring, industrial control, and healthcare, smart mobile devise etc. Sensors permit measurements of environmental parameters done in a context sensitive fashion, and facilitate the device for interacting with people living in surroundings and physical world.

Connectivity: Various technologies are utilized for building connectivity among internet andIoT devices, facilitate availability of service, information interchange globally, and communication between different infrastructures.

Intelligence: Data collection and sensing are enabled in IoT devices. Various algorithms are included in that for making decisions and facilitating smart data analysis.

Heterogeneity: In IoT, different operating systems and hardware platforms are used. This sophisticated system has to permit interconnection between services and non-homogeneous devices for yielding data exchange seamlessly.

Dynamic modifications: IoT networks are defined using topology changes happening dynamically, as they are allowed to connect or disconnect based on their mobility or power of battery. In addition, rising IoT devices count and their application invokes more dynamicity in the network topology.

Scale: A huge amount of IoT devices produce a magnanimous data. This implies that the management of network and data analysis to become a big challenge and needs scalable IoT approaches and solutions

3. Information-Centric Networks (ICN)

Information-Centric Networking [22] is introduced in the form of a novel architecture for the Internet in the future, dealing with several challenges in the present IP-based networks, like routing procedure, scalability problem, and the performance of content sharing [24]. ICN combines all the functionalities of the network built around the name of content instead of the network address, in a means to guarantee effective data distribution and access.

Earlier, various concepts like P2P and CDN are designed for boosting sharing as well content distribution in Internet [25]. In addition, ICN is a standardized protocol in contrary with CDN and P2P and, and it works at network layer. P2P is an application-specific protocol; CDN is a licensed solution operating in the application layer. Also, P2P content delivery is done from end-users, but CDN uses licensed infrastructure. But, ICN delivers the content using network infrastructure.

This mode of redesigning arising from ‘‘where is content” to ‘‘what constitutes content’’ will help in improving performance of network, enable content recovery as well as duplication using in-network content caching, and providing support to mobility and native multicast delivery.

Fig. 2 shows difference between ICN and IP communication. Red and blue color is used for representing the Content retrieval correspondingly. Presuming that all the users are asking for the same content *D*rendered by producer, communication based on IP needs every client is aware of content generator address, and gets the content via an IP routed path. But in communication based on ICN the client smustmention requested content name (with no knowledge of the host IP). Request is forwarded depending on rules of name-based routing until it gets to a device with content. As per Fig. 4, the client 3’s request is fulfilled by generator, during which router can have content cached. When client 4 asks same content, then request is met by cache store at R3, thereby avoiding reaching actual generator task.

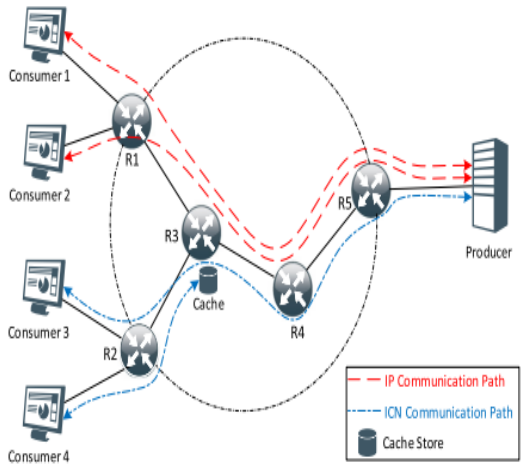

Figure 2. Content Retrieval: IP-based vs. ICN-based Networks

Several technical works have highlighted on various functionalities of ICN like security, mobility, in-network caching and caching.

4. Why ICN for IoT?

The data delivered by IoT keen gadgets can be viewed as substance [26]. Customers in the system demand information in IoT setting without the need to know the area of the sensors or the actuators. There is no closure to-end meeting necessity for content recovery, and ICN focuses on the substance in the system by its name as opposed to its location. For instance, requesting moistness esteem for a particular spot, or inquiry some data, or information checking.

ICN hubs can go about as imitation hubs by utilizing content stores. Substance can be reserved and served for future demands paying little mind to the first maker's reach ability. This reserving improves the information recovery, and lessens the idleness. In such situations, ICN is more appropriate for IoT than IP [27], for the quick substance conveyance, yet additionally for it get driven plan and solicitation accumulation. Also, multicast and versatility backing of ICN is an added substance point, where multicast should be possible from the system layer, and any unsatisfied solicitations during portability can be re-given without the requirement for complex handover arrangements like those of IP. Besides, by utilizing worldwide one of kind names, ICN gives content-based security and encryption, and guarantees content honesty and legitimacy, as a feature of its plan. IoT can be joined with various every day client schedules, by empowering consistent coordination and communication with applications, sensors, and actuators. Day by day close to home checking, modern procedures controls are some genuine instances of IoT applications. By utilizing content-based naming and Name Resolution System (NRS), the tending to issue in IoT can be explained. This will likewise help in expelling any limitation on the kind of substance and the idea of maker gadget [28].

Also, separating content from actual location, and utilizing name in form of primary element for identifying the content, the non-homogeneous characteristics of IoT sensors holds no relevance [29]. From security point of view, communication channel security in ICN is unnecessary since latter adopts a content-based technique through content encryption itself and using diverse trust models in application layer. Also, as IoT devices are limited in resource, session-less concepts, interest aggregation, caching placement/replacement frameworks, forwarding mechanisms, and in-network caching helps in improving energy efficacy as well as minimizes power usage. On the whole, all these characteristics have a major role in making ICN an effective alternate solution of IoT with respect to flexibility and robustness [30].

5. Related Works

Many research works are available in literature which deals with ICN and IoT individually. These attempts are summarized below for the reader's perusal. Sheng et al. [31] introduced various communication standards by providing a review on the IoT solutions in industrial as well as academic point of view, focusing on key problems in massive-scale IoT networks.

5.1 Survey Highlights on ICN (i.e. CCN and NDN Frameworks) in IoT Applications

Network architecture named Keyword-Based Content Retrieval (KBCR), which is a ICN extension, is proposed in [32] for IoT applications. KBCR node will spreads a greater number of requests to the data having relation with received keyword request. If multiple responses are received in this node, then single response is formed by merging those multiple responses. Over network, in a tandem manner, on multiple nodes, this process is carried out. A single aggregated response is given to requester and it will reduce number of response or request messages. The KBCR concept is described in this paper, which is used in IoT applications. Numerical analysis is presented for showing efficiency of proposed method.

In [33] centre around the reserve portion issue, in particular, how to circulate the store limit across switches under a compelled all out capacity spending plan for the system. We initially detail this issue as a substance situation

issue and acquire the ideal arrangement by a two-advance strategy. We at that point propose a problematic heuristic strategy dependent on hub centrality, which is progressively down to earth in unique systems with visit content distributing. We research through re-enactments the components that influence the ideal reserve allotment, and maybe more critically we utilize a genuine Internet topology and video get to logs from a huge scope Internet video supplier to assess the presentation of different store distribution strategies. Also, the heuristic technique exhibits quite constrained performance penalty in comparison with the optimum allocation. At last, with the help of the inferences, recommendations are provided for network operators for deploying the CCN caches capacity over routers in the best way.

Xu et al. [34] implemented an information-centric multimedia streaming method, which is energy efficient in vehicular networks (GrIMS). In wireless vehicular ad hoc networks (VANETs), which are heterogeneous, multimedia retrieval is characterized using a multiple windows' queuing model having differentiated service rates. In order to make a balance between qualities of experience (QoE) and energy efficiency, cost optimization model is modelled by authors. Because of time varying conditions like vehicle mobility, it is infeasible to solve those models practically in real time conditions. In network caching context, multipath selection and GrIMS's cloud-based processing, for saving energy and achieving high level of QoE, heuristic algorithms set is proposed by the authors.

In VANETs, for multimedia delivery, cooperative caching solution based on ICN is proposed in [35]. In highway, for enhancing coaching resources utilization, potential social cooperation between neighbour vehicles are explored in this paper. With multiple lanes, highway traffic model is proposed by authors and two classes of vehicle like couriers and partners are considered in cooperative coaching based on social context and information about lane and location. Without excessive delay in start-up, quality of video playback is maximized in this proposed model with minimized ratio of playback freezing.

Femminella et al. used distributed caching for implementing an architecture which is used for dynamic sensor data distribution [36]. Network nodes virtualization and service modularization are performed using NetServ hosting environment. Network nodes functions are extended using this implementation. At all-time huge number of software or recipients' components are allowed to access the information which is collected from huge number of distributed sensors. For example, fault recovery, security engines, augmented reality server's applications. In overall network and latency, downward trend is indicated in simulation results.

Various replicating or caching genome data set insight is provided in [37]. Genome content distribution is optimized and enhanced using those provides guidelines. Main genome processing applications are analysed by authors and alternatives of genome workflow computations are classified into distributed cloud or location machine. Major networking topologies available are also discussed for effectively supporting solutions of genome as a service (GaaS). Genome content popularities temporal evolution difficulties are highlighted in this paper and for data storage management, various suggestions are given, which can be utilized to distribute genomic content in an optimized way.

Anticipating popularity variations can be allowed between various datasets by discovering hidden relationship between them as argued by authors. Geographically distributed replicas management is facilitated using this relationship. In genome data caching, issues of privacy and security are also discussed. For anonymized contents, it is feasible to cache or replicate genomic dataset because of personal information availability in genome data for which issued an informed consent.

In order to make specific service requirements of a dynamic condition-based decisions, artificial intelligence (AI) model needs to be performed by IoT devices because of Internet of Things (IoT) network's rapid development. Large amount of caching, computing and communication resources are needed for using and generation of AI model. So, network construction and limited network resources scheduling for realizing AI model's propagation and rapid generation of AI model are difficult.

Information Centric-Internet of Things (IC-IoT) architecture which is defined using software is proposed in this model for bringing computing and caching abilities to IoT network [38]. In order to manage caching and computing resource uniformly, joint resource scheduling method is designed using proposed IC-IoT architecture.

Reward maximization is a major objective, where it has both long term reward as well as short term reward. Popular AI models are cached for creating long term rewards. Multi-dimensional optimization problem is formulated from resource scheduling problem. But it is highly complex and in high dimension. So, to avoid this, proposed a new deep Q-learning. Iot in resource allocation method and IC-IoT architecture defined by software's effectiveness is verified in simulation results.

Xiaohu Chen et al. [39] implemented as caching method for delivering content in Information-Centric Network, which is termed as Least Unified Value (LUV)-Path. For demonstrating, cooperatively and collectively cached contents of router and whole path of delivery, unique value is assigned in proposed method. This value is termed as LUV and, in order to show its importance, it is combined with the distance between content provider and router.

Under various topologies, LUV Path concept is implemented by authors and using LUV Path technique in LUV, LRU, FIFO algorithms, alleviating provider pressure, traffic in network and customer delay are reduced as proven by authors. Content popularity distribution scope is

introduced by them for extending future work for providing host judgement for propagating contents in network at reduced retrieval delay and redundancy.

Xiaoyan Hu et al. [40] implemented as routing method for providing caching in routing and name based methods. Cache systems based on knowledge are focused majorly in this system, where, for guaranteeing caching in control plane using self-awareness is provided using Cache-Aware Name Based Routing (CANR) technique. The kind of content has to be cached and kind of information has to be advertised to the network needs be learned by router in this method. Every router caching need is estimated and calculated using Import Cache Filter Model (ICFM). In network, caching routing information advertisement is done using Export Cache Routing (ECR), which tends to provide scalability of system.

KyiThar et al. [41] implemented a cooperative caching and forwarding technique based on consistent hashing in centric network. In maintaining network's storage capacity and cache redundancy, optimum performance is not shown in Leave Copy Everywhere method of caching. Router virtualization is major concentrated in that approach, where, interest packets are forwarded using multiple router groups and data is cached collectively using them. Modulo hashing is used for proposing solution to the problem of scaling, but, for cache replacement and decision, prediction of content popularity is still a difficult task.

In Software defined information centric networking (SD-ICN), for addressing the problem of control plane scalability, for intra-domain communication, scalable area-based hierarchical architecture (SAHA) is proposed in [42]. Content and network resources, scalable awareness is supported using SAHA and adaptation of resources and efficient matching of interest are also guaranteed using this model.

5.2 Survey on Data Storage, Retrieval with De-duplication, Memory Handling and Encryption Performance

Chen et. al [43] used convergent key management model for providing security in duplication. In this model, master key is hold by cloud user for encrypting convergent key and in cloud it is stored. When there is an increase in cloud user, number of keys generated is also increased in this independent master key management model. So, users are forced in this independent master key management model to predict master key of their own. A novel method is implemented in this paper, which permits the user to store their master in various servers instead keeping it with them. Ramp Secret Sharing method is used for implementing Dekev system, because of that, system security is enhanced as shown in the results of experimentation.

Jiang et al., [44] constructed a Disjunctively Oblivious Keyword Search (DOKS) protocol, which is an effective and efficient one and it permits short cipher text and fast search. On cloud storage provider and user side, high privacy is provided using this model. When compared with Oblivious Keyword Search (OKS) protocols, less storage and computation space is needed in DOKS protocol and better efficiency and privacy is given using this protocol. Two search keywords having interrelation are submitted by user and relationship between search keyword and documents cipher text needs to be known by user. On search query, statistical information can be revealed without matching documents retrieve but multi-keyword search is not supported in this model.

Lu et al., [45] constructed a Logarithmic Search over Encrypted Data (LSED) system by designing cryptographic primitive - range predicate encryption model. Following are the features of this system. Secured data update, authentication of query, support to logarithmic search in encrypted data, privacy predicate, confidentiality of plain-text. Cipher texts access patterns are revealed using LSED system to cloud server. Owner of database defines update operation of database; authorization of query and they are the single failure point.

A secret is used in an effective MPEG video encryption algorithm [46]. The I picture's DC coefficients differential values in encoded forms sign is changed randomly in this technique. B and P frames motion vectors encoded differential values and I fames AC coefficients sign bits are unchanged. On demand video, video email and video conferencing are secured fast using this VEA with minimized encryption complexity.

A chaos based selective encryption approach [47] has been introduced on the H.264/AVC standard. For masking the chosen H.264/AVC syntax components, four digitized Renyichaostic maps used for generating a pseudorandom bit sequence. The newly introduced algorithm exhibits high sensitivity to the secret key and yields good perceptual security. The novel algorithm yields a format compliant, quick and secure H.264/AVC video sequences selective encryption by damaging their commercial intent.

JagdishPatil et al. [48] presented a compact block cipher approach known as LiCi. An encryption method, which employs a 128-bit key for encrypting the 64-bit plaintext, to generate the 64-bit cipher is proposed. 4-bit input and 4-bitoutput S-box is used. It splits the 64-bit plain text into two equal parts. From 128-bit key, it pulls out the left most significant bits and utilizes them as the first-round key, and the next left most significant bits are utilized in the form of second round key. LiCi approach includes 31 rounds.

Novel solution was assessed on various parameters like cycles count, throughput, execution time, key size and block size. The comparison of LiCi cipher was also done with other small ciphers based on hardware performance such as power usage, flash memory employed and GE, s.LiCi uses

1944 bytes memory and it needs 1153 GE, s (GateEquivalents) for encrypting data of 64- bit using a key of 128-bit. LiCi cipher takes up 30mW power, which is quite less in comparison with other available approaches. It is resilient against the linear and differential attacks.

Manish Kumar etal. [49] Proposed a dynamic key technique for securing the Internet of Things. In the recent times, an important field of interest in the data security of digital world in the form of IoT, where devices communicate among themselves. It simplifies human life but the security of the data that they generate is a problem. The novel dynamic key scheme was symmetric key encryption. It uses a 128-bitkey, which is resistance against brute force attack. It considers 8 bytes data as input and produces a fixed 8 bytes cipher-text in output form. This makes sixteen sub keys of8 bits using the 128-bit key.

So, the shuffling process is utilized for acting against the popular plain text attack, and finally, the diffusion process is utilized for avalanche effect. The novel solution was verified on diverse negative features such as dissimilar keys for encryption and decryption, a small variation of key, a smallvariation of plain text, and incorrect ciphertext. The results have revealed that the model was capable of detecting all these marginal changes and its ciphertext could not get decrypted. The system was capable of identifying the minor changes. The key length was sufficient to safeguard it from brute force attack. It employed an equal number of bits in the output ciphertext and input plaintext, to help saving the network bandwidth.

Hong Liu et. al [50] have considered the privacy challenges in cloud storage systems and introduced a Shared Authority based Privacy preserving Authentication (SAPA) protocol where a novel mechanism where, request of anonymous data access is compared data storage systems privacy and security. In addition, storage technique is added with access control based on an attribute for reminding the user that they can have access to just their own data. During the processing of these anonymous requests, proxy re-encryption is used since the data is shared among a number of users in the cloud. This shows that this technique fascinates companies for multi-client coordinated cloud applications.

6. Inference from the Existing Work

This section explores ICN-based naming approaches which are introduced and tested for IoT applications. The ICN-based naming approaches for Io T are categorized into four groups, which include hierarchical, flat self-certifying, attribute based and hybrid naming approaches. This survey shows that for IoTs, named data networking (NDN) (CCN) hierarchical naming approaches and hybrid naming approaches have achieved more focus from the research community in comparison with flat and attribute-based naming methods

It is observed that the primary reasons behind NDN (CCN) hierarchical naming possibility for IoTs include its simplicity and easier name-aggregation and remarkable support for scalability. In addition, human-interpretable hierarchically structured names having infinite length yields rapid searching in comparison with other approaches and also name-aggregation helps saving a good amount of space while simplifying the routing.

Then again, ICN-based hybrid naming approaches improve the advantages of combined naming approaches. A hierarchical component is included with the objective to yield scalable and effective name aggregation with lesser number of entries to simplify the routing process. The flat-name component is added to guarantee enhanced privacy and security. Contents attributes are also included to make deep learning techniques searching feasible using attribute keywords.

The research challenges include

- Caching in information centric nodes results in improved number of duplications that might result in more computational overhead
- Storage and retrieval of the multimedia contents from IoT devices would result in memory storage overhead being increased which has to be focused in the novel research technique
- Security of the multimedia files to be transmitted is complicated to guarantee in case of more amount of contents being available
- The abovementioned challenges have to be highlighted in the proposed research approach for having a superior performance.

Table 1. Comparison of Available Techniques

Author	Technique	Objective	Results
ICN (i.e. NDN and CCN architectures) from IoT applications			
Sheng et al (2013)	Scalable area-based hierarchical architecture (SAHA) of intra-domain communication	SAHA provides support for scalable sensitivity of network and resources of content, and usage of resources and effective matching of interest are also ensured.	Hugely needed by IoT since both fixed and mobile devices can be added.
Saxena et al	Keyword-Based Content Retrieval (KBCR)	One single response is formed by merging multiple response that the node gets. All over the network,	The newly introduced mechanism is assessed, in terms of resource

(2016)		in a tandem manner, in multiple nodes, performed this process. Therefore, merged data is delivered to a requester in just one response and minimized number of request/response messages.	efficiency and QoS metrics in practical workload circumstances.
Data Storage, Retrieval with Deduplication, Memory Handling And Encryption Performance			
Chen et. al (2014)	Deduplication by convergent key management approach	A new technique (Dekev) where the users are no longer forced to have their master keys stored with themselves and instead, they are stored across different servers.	Improved security of the system
Hong Liu et. al (2015)	Shared Authority based Privacy preserving Authentication (SAPA) protocol	SAPA to deal with above privacy challenge for cloud storage.	The novel protocol is applicable for multi-user collaborative cloud applications.
Lui and Wong (2013)	Chaos based selective encryption approach	Used for the generation of a pseudorandom bit sequence having maximum security	The novel algorithm exhibits high sensitivity to the secret key and has good perceptual security.

7. Solution

In networks Content delivery between the content request generators(subscribers) and the server (publisher) in the Internet of Things (IoT) environment involves the future Internet, known as Information-Centric Networking (ICN), due to caching contents by in-network nodes. In ICN caching, every network node is capable of storing contents locally. If a subscriber requests a specific content, a copy of the requested content is stored by local network node(s). Therefore, subsequent requests for the same content may be satisfied locally. Deduplication may perform by creating indexing table for each data using deep learning model to avoid computational overhead. All nodes can be clustered within the communication range and select cluster head to increase the energy efficiency. And also cloud-based application delivery(CBAD) platform could be used to provide security against all kinds of attacks for this video and audios.

8. Results and Discussion

The proposed work, is implemented using NS2 simulator. The simulator is installed on a machine that is running Ubuntu 16.04 operating system. The topology consists of 40 ICN nodes, which are randomly placed in an area of 100m x 100m. In the simulation setup, one node is designated as the publisher that runs IEEE802.15.4 Zig-Bee protocol, whereas the remaining 39 nodes function as subscribers that run the IEEE802.11a WiFi standard .The cache size of every node is set to accommodate 5 chunks in one scenario and 10 chunks in the second scenario that are simulated in 100 different runs.

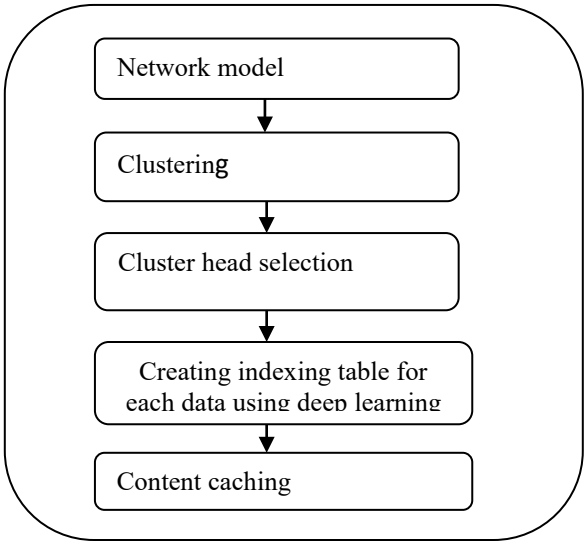

Figure 3. Overall flow of the proposed work

The Zipf popularity model is selected with the _ value ranging from 0.5 to 1. Every time the topology is simulated for 120 seconds wherein the average of all 100 runs is combined as a final result. And in this section proposed model is compared with the existing methods to show the efficiency of the model in terms of energy efficiency, bandwidth consumption, Attack detection accuracy.

Table 2. Experimental environment; parameters and values

Parameter	Description
Popularity model	Zipf
A	0.5,0.6,0.7,0.8,1

Simulation area	100 × 100 m
Wireless connectivity	Zig-Bee, Wifi
Publisher	1
Subscribers	39
Cache size	5,10 chunks
File size	Chunks
Frequency/sec on invidual messages	8 -10/sec
Mobility model	Random direction
No. of simulation runs	100
Simulation time/run	120 sec

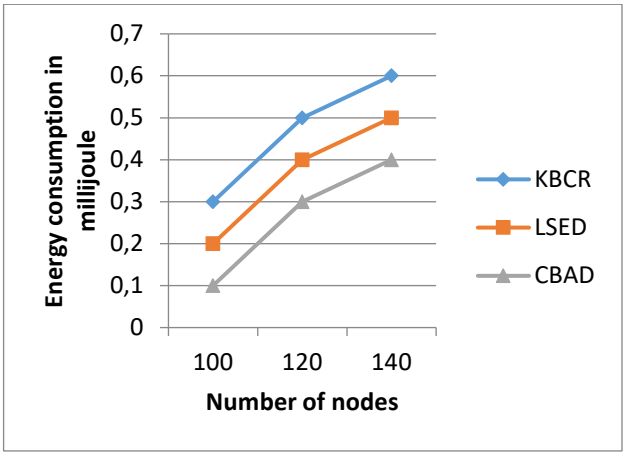

Figure 4. Comparison between Energy consumption (mj) and number of nodes

Figure.4 illustrates the comparison performed Comparison between Energy consumption and number of nodes of the novel CBAD and the already available KBCR, LSED methods. It is concluded that the proposed CBAD yields a much better Energy consumption in comparison with the available KBCR, LSED methods.

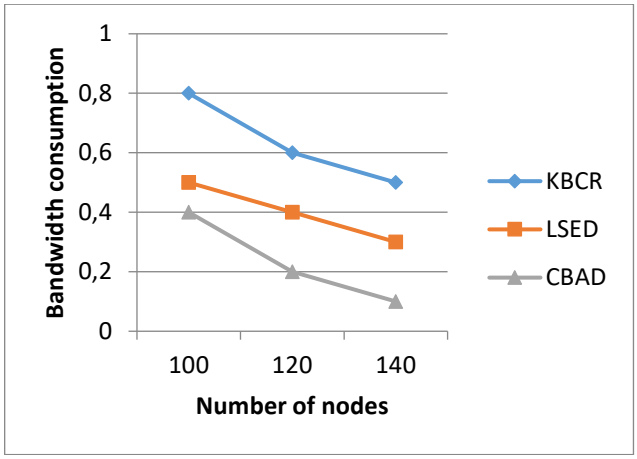

Figure 5. Comparison between the bandwidth consumption and number of nodes

Figure.5 illustrates the comparison performed between the bandwidth consumption and number of nodes of the novel CBAD and the already available KBCR, LSED methods. It is concluded that the proposed CBAD yields much better bandwidth consumption in comparison with the available KBCR, LSED methods.

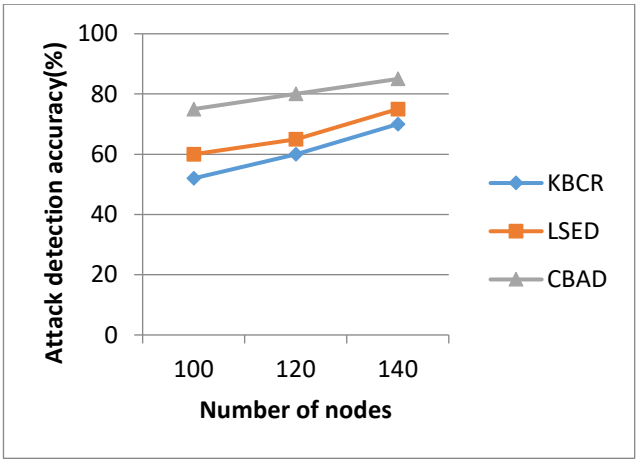

Figure 6. Comparison between the Attack detection accuracy (%) and number of nodes

Figure.6 illustrates the comparison performed between the **Attack detection accuracy and number of nodes** of the novel CBAD and the already available KBCR, LSED methods. It is concluded that the proposed CBAD yields a much better network **Attack detection accuracy** in comparison with the available KBCR, LSED methods.

9. Conclusion

The conventionally designed network architecture for IoTs is considered for connecting very a smaller number of computers and sharing less and in-economic network resources using the restricted address space at the network layer, it is surely not developed for meeting the demands of IoTs. In order to satisfy these IoTs requirement, Information-Centric Networking (ICN) is presently evolved as a suitable solution. But, in spite of multiple contributions made, ICN-based IoT caching encounters multiple issues. This article reviews the caching challenges faced in the ICN-based IoT environment presented in recent works. And finally concludes that the deduplication based on index table using deep learning and also cloud-based application delivery (CBAD) platform could be used to provide security and energy efficient content delivery.

References

[1] Ierc-european research cluster on the internet of things. [Online]. Available: http://www.internet-of-things-research.eu/about-iot.htm

[2] Atzori, L., Iera, A., &Morabito, G. (2010). The internet of things: A survey. *Computer networks*, vol.54, no. 15, pp. 2787-2805.

[3] Gubbi, J., Buyya, R., Marusic, S., &Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, vol. 29, no. 7, pp. 1645-1660.

[4] Shang, W., Yu, Y., Droms, R., & Zhang, L. (2016). Challenges in IoT networking via TCP/IP architecture. *Technical Report NDN-0038. NDN Project*, pp.1-7.

[5] Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, vol. 54, no. 1, pp. 1–31.

[6] Stankovic, J. A. (2014). Research directions for the internet of things. *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3-9.

[7] Varadharajan, V., &Bansal, S. (2016). Data security and privacy in the internet of things (iot) environment. In *Connectivity Frameworks for Smart Devices*, pp. 261-281.

[8] Silva, R., Silva, J. S., &Boavida, F. (2015). Infrastructure-supported mobility in wireless sensor networks—a case study. In *2015 IEEE International Conference on Industrial Technology (ICIT)* ,pp. 1895-1900.

[9] Al-Nidawi, Y., Yahya, H., & Kemp, A. H. (2015). Impact of mobility on the IoT MAC infrastructure: IEEE 802.15. 4e TSCH and LLDN platform. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pp. 478-483.

[10] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., &Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys &tutorials*, vol.17, no. 4, pp. 2347-2376.

[11] Named data networking (ndn) project. [Online]. Available: http: //named-data.net/

[12] Pursuing a pub/sub internet-fp7 project pursuit. [Online]. Available: http://www.fp7-pursuit.eu/PursuitWeb/

[13] Network of information (netinf). [Online]. Available: http://www. netinf.org/

[14] Comet project overview. [Online]. Available: http://www. comet-project.org/overview.html

[15] Fp7convergence project. [Online]. Available: http://www. ict-convergence.eu/

[16] Mobilityfirst future internet architecture project. [Online]. Available: http://mobilityfirst.winlab.rutgers.edu/

[17] (2016) Cyber-secure data and control cloud for power grids. [Online]. Available: http://cdax.eu/

[18] (2016) Greenicn architecture and applications of green information centric networking. [Online]. Available: http://www.greenicn.org/

[19] The ccnx project. [Online]. Available: http://blogs.parc.com/ccnx/

[20] Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., &Ohlman, B. (2012). A survey of information-centric networking. *IEEE Communications Magazine*, vol.50, no.7, pp. 26-36.

[21] Xylomenos, G., Ververidis, C. N., Siris, V. A., Fotiou, N., Tsilopoulos, C., Vasilakos, X., ... &Polyzos, G. C. (2013). A survey of information-centric networking research. *IEEE communications surveys &tutorials*, vol. 16, no.2, pp. 1024-1049.

[22] Amadeo, M., Campolo, C., Iera, A., &Molinaro, A. (2015). Information centric networking in IoT scenarios: The case of a smart home. In *2015 IEEE international conference on communications (ICC)*, pp. 648-653.

[23] Fotiou, N., &Polyzos, G. C. (2014). Realizing the internet of things using information-centric networking. *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*,,pp. 193-194.

[24] Qiu, L., Padmanabhan, V. N., &Voelker, G. M. (2001). On the placement of web server replicas. In *Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society,* pp. 1587-1596.

[25] Cronin, E., Jamin, S., Jin, C., Kurc, A. R., Raz, D., &Shavitt, Y. (2002). Constrained mirror placement on the Internet. *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 7, pp. 1369-1382.

[26] Baev, I. D., &Rajaraman, R. (2001). Approximation algorithms for data placement in arbitrary networks. In *Proceedings of the twelfth annual ACM-SIAM symposium on Discrete algorithms* pp. 661-670.

[27] Loukopoulos, T., & Ahmad, I. (2004). Static and adaptive distributed data replication using genetic

algorithms. *Journal of Parallel and Distributed Computing*, vol.64, no. 11, pp. 1270-1285.

[28] Yang, M., &Fei, Z. (2003). A model for replica placement in content distribution networks for multimedia applications. *IEEE International Conference on Communications,* pp. 557-561.

[29] Yu, H., &Vahdat, A. (2002). Minimal replication cost for availability. *Proceedings of the twenty-first annual symposium on Principles of distributed computing*, pp. 98-107.

[30] Zhuo, L., Wang, C. L., & Lau, F. C. (2002). Load balancing in distributed web server systems with partial document replication. In *Proceedings International Conference on Parallel Processing*, pp. 305-312.

[31] Sheng, Z., Yang, S., Yu, Y., Vasilakos, A. V., McCann, J. A., & Leung, K. K. (2013). A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. *IEEE wireless communications*, vol. 20, no. 6, pp. 91-98.

[32] Kurita, T., Sato, I., Fukuda, K., &Tsuda, T. (2017). An extension of information-centric networking for iot applications. In *2017 international conference on computing, networking and communications (ICNC)*, pp. 237-243.

[33] Wang, Y., Li, Z., Tyson, G., Uhlig, S., &Xie, G. (2015). Design and evaluation of the optimal cache allocation for content-centric networking. *IEEE Transactions on Computers,* vol. 65, no. 1, pp. 95-107.

[34] Xu, C., Quan, W., Zhang, H., &Grieco, L. A. (2016). GrIMS: Green information-centric multimedia streaming framework in vehicular ad hoc networks. *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 2, 483-498.

[35] Quan, W., Xu, C., Guan, J., Zhang, H., &Grieco, L. A. (2014). Social cooperation for information-centric multimedia streaming in highway VANETs. *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks,* pp. 1-6.

[36] Femminella, M., Reali, G., Valocchi, D., Francescangeli, R., &Schulzrinne, H. (2013). Advanced caching for distributing sensor data through programmable nodes. *IEEE Workshop on Local & Metropolitan Area Networks (LANMAN)*, pp. 1-6.

[37] Reali, G., Femminella, M., Nunzi, E., &Valocchi, D. (2018). Genomics as a service: A joint computing and networking perspective. *Computer Networks*, pp. 27-51.

[38] Xu, F., Yang, F., Bao, S., & Zhao, C. (2019). DQN inspired joint computing and caching resource allocation approach for software defined Information-Centric Internet of things network. IEEE Access, pp. 61987-61996.

[39] Chen, X., Fan, Q., & Yin, H. (2013). Caching in Information-Centric Networking: From a content delivery path perspective. *International Conference on Innovations in Information Technology (IIT)*, pp. 48-53.

[40] Hu, X., & Gong, J. (2014, November). CANR: Cache-Aware Name-based Routing. *International Conference on Cloud Computing and Intelligence Systems*, pp. 212-217.

[41] Thar, K., Ullah, S., & Hong, C. S. (2014). Consistent hashing based cooperative caching and forwarding in content centric network. *Asia-Pacific Network Operations and Management Symposium*, pp. 1-4.

[42] ZSheng, Z., Yang, S., Yu, Y., Vasilakos, A. V., McCann, J. A., & Leung, K. K. (2013). A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. *IEEE wireless communications*, vol. 20, no. 6, pp. 91-98.

[43] Li, J., Chen, X., Li, M., Li, J., Lee, P. P., & Lou, W. (2013). Secure deduplication with efficient and reliable convergent key management. *IEEE transactions on parallel and distributed systems*, vol. 25, no. 6, pp. 1615-1625.

[44] Jiang, Z., & Liu, L. (2013, June). Secure cloud storage service with an efficient doks protocol. *IEEE International Conference on Services Computing*, pp. 208-215.

[45] Lu, Y. (2012, February). Privacy-preserving Logarithmic-time Search on Encrypted Data in Cloud. In *NDSS*,

[46] Shi, C., &Bhargava, B. (1998). A fast MPEG video encryption algorithm. In *Proceedings of the sixth ACM international conference on Multimedia* pp. 81-88.

[47] Lui, O. Y., & Wong, K. W. (2013). Chaos-based selective encryption for H. 264/AVC. *Journal of Systems and Software*, vol.86, no. 12, pp. 3183-3192.

[48] Patil, J., Bansod, G., & Kant, K. S. (2017). LiCi: A new ultra-lightweight block cipher. In *2017 International Conference on Emerging Trends & Innovation in ICT (ICEI)*, pp. 40-45.

[49] Kumar, M., Kumar, S., Budhiraja, R., Das, M. K., & Singh, S. (2016). Lightweight data security model for IoT applications: a dynamic key approach. In *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 424-428.

[50] Liu, H., Ning, H., Xiong, Q., & Yang, L. T. (2014). Shared authority based privacy-preserving authentication protocol in cloud computing. IEEE Transactions on parallel and distributed systems, vol. 26, no. 1, pp. 241-251.

[51] Mahaveerakannan, R., and Dr. C Suresh GnanaDhas. "Big data analytics for large-scale UAV-MBN in quantum networks using efficient hybrid GKM." CONCURRENCY AND COMPUTATION-PRACTICE & EXPERIENCE (2019).

[52] Mahaveerakannan, R., and Dr. C Suresh GnanaDhas. "Cloud-Based Healthcare Portal in Virtual Private Cloud." Inventive Communication and Computational Technologies, Springer (2020).