International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 477-484 June 2018-Dec 2018 www.csjournals.com

A Privacy Preserving Based Data Centric Networks Employing Caching Technique

Khaja Fareeduddin Umair [1], MD Ateeq Ur Rahman [2]

[1] Research Scholar, Dept. of Computer Science & Engineering, SCET, Hyderabad
umair.ameen95@gmail.com
[2] Professor and Head, Dept. of Computer Science & Engineering, SCET, Hyderabad
mail_to_ateeq@yahoo.com

Abstract: Content-Centric Networking (CCN) is a web structure for transferring titled proportionality from producers to consumers upon missive. The name-to-content binding is cryptographically implemented with a digital melody generated by the shaper. Thusly, content unity and source credibility are core features of CCN. In opposition, cognition confidentiality and isolation is sect to the applications. The typically advocated coming for protecting sensitive noesis is to use encryption, i.e., control make to those who mortal suitable cryptography key(s). Moreover, proportion is typically encrypted for same requests, meaning that umpteen consumers obtain the said encrypted activity. From a concealment perspective, this is a block backwards from the "essay, we set the isolation pitfalls of this approach, especially, when the antagonist learns several auxiliary aggregations around popularity of indisputable plaintext proportionality. Simply by observing (or learning) the rate of requested knowledge, the human can discover which encrypted corresponds to which plaintext data. We valuate this start using a custom CCN simulator and evince that symmetrical somewhat surgical popularity message suffices for straight correspondence. We also demonstrate how the opponent can apply caches to hear noises popularity aggregation. The soul needs to copulate the accumulation namespace in organization to succeed. Our results impart that encryption-based gain criterion is meagerly for reclusiveness in CCN. Author abundant counter-measures (such as namespace restrictions and acceptance replication) are necessary to mitigate the onslaught.

1. INTRODUCTION

Information-Centric Networking (ICN) is a new networking family that treats volume (aka information or info) as a first-class target. Content-Centric Networking (CCN) is a limited typewrite of request-based ICN where a consumer fetches collection by issuance a declared quest (called a recreation) that refers to t e wanted activity by figure. The fabric is causative for routing interests towards either a producer of that collection or a router that has previously cached it. At every router hop, per-interest commonwealth is socialistic behind To allot the accumulation to be dispatched indorse, along the aforesaid course, thusly preventive the pauperization for a "seed destination" in a worry. Moreover, every router along the way is release to opportunistically store proportionality in inflict to provide ulterior interests. Consequent interests that ask for the very aggregation (by the like itemize) may termination in thing state served from any moldiness be autographed by its shaper. In counterpoint, as network-layer architecture, CCN does not dominion cryptography: thing is transferred in clear text, unless previously encrypted above the textile layer. Thus, it is insignificant to eavesdrop on obloquy carried in interests and corresponding content payload. If noises payload is encrypted, then exclusive the knowledge denote is leaked. Ghazi et al. [11] freshly showed that, in condition to lessen this more leakage, the jargon contained in a concern moldiness be the production of an adjusted deterministic pseudorandom work (PRF) Fake (·). This way, two consumers who communicate the identical knowledge with factual canonized) consumers.

Eavesdroppers then exclusive acquire that two consumers message the comparable content, and not it’s actualized folk. Ghazi et al. also converse in [11] that the above is low from a reclusiveness perspective. In primary, if the opponent has more help substance nigh the requested activity e.g., its popularity within a supposal namespace, it can recuperate the accumulation analyze flush if PRF-transformed names are utilized. The cogitate is due to percentage likability, i.e., knowledge to conclude when two interests touch to the individual can discover entropy active inexplicit interests based on their PRF-transformed defamation. This write of leakage is not incomparable to CCN. If we deliberate CCN as a generic key-value outlet where PRF-transformed interests are keys, and proportionate volume packets are values, the problem at laborer is similar to reclusiveness leakage in encrypted databases. This topic has been extensively deliberate in recent years [27]. In this paper, we hold to CCN attacks from the search literature ICN '17, Sept 26-28, 2017, Songwriter, Germany Cesar Ghazi, Factor Studio, and Christopher A. Actress

On isolation of encrypted databases. Specifically, we document adversarial cognition to see plaintexts of requests and responses using exclusive aggregation scholarly from eavesdropping on encrypted interchange.

In doing so, we try to answer the following questions:

- How does the truth of opposer's helper entropy work effectualness of privacy attacks?
- How does router caching concern attacks, and how does it link to topological dispersion of the resister?
- Can replicating or analysis proportionality among denary producers modification effectualness of these attacks, and if so, to what qualification?

II. PRELIMINARIES

Assemblage Central Networking (CCN) is a striking ICN architecture, originally mature at PARC. Titled Aggregation Networking (NDN) [36] is its pedantic dual. CCN and NDN person pardonable prescript and packet split differences. In this material, we absorption primarily on the plate.This part overviews CCN with honor to the latest specifications [24] and the CCN publication feat. Presented intimacy with either CCN or NDN, it can be skipped without disadvantage of
Strength. In differ to IP, which focuses on end-points of act and their names and addresses, CCN [13, 24] focuses on proportion by making it titled, addressable, and routable. Acceptance kinfolk are a URI-like [3] progress dignified of one or author variable-length segments. To obtain aggregation, a soul (consumer) issues a substance, called a portion message, with the analyze of the desired cognition. A recreation can be mitigated by either: (1) a router storing requested cognition in its stock, or (2) the noesis shaper. In either casing, a noesis target message is returned to the consumer. (If a shaper cannot cater or NACK [7].)

Substance from the name, portion messages may let the stalking elective fields:

Payload - an installation that lets consumers push data to producers along with the share.

KeyId Restriction - hash of the people key utilized to swan desirable proportionality's tune. If submit, CCN guarantees that only acceptance objects that can be verified with the nominal key are returned in salutation to an portion.

Content Object Hash Restriction - hash of the assemblage beingness requested. If instant, CCN guarantees conveyance of accumulation the hash of which matches the consider of this installation.

Substance objects ever disperse a load (i.e., the actualized cognition) and many further metadata. Different interests, they also commonly disseminate an authenticator, i.e., a manner or a Communication Proof Code (MAC). An authenticator is victimized to behave correctness of name-to-content cover, and it allows consumers and routers to swear legitimacy and state of returned activity. Volume objects do not demand to gestate a nominate if the corresponding concern included a Content Object Hash Restriction land. This is because the volume can be twin to the interestingness by technology and checking that its hash equals the corresponding facility in the touch. (This tab is victimised to authenticate the response.) There are trey types of entities in CCN:2 (1) consumer, which issues interests for volume, (2) maker, which generates and publishes proportion, and (3) routers, which assumptive.

Forwarding Interest Base (FIB) – table of name prefixes and corresponding outgoing interfaces. The FIB is used to route interests based on longest-prefix-matching of their names.

- Pending Interest Table (PIT)–table of outstanding (pending) interests and, for each, a set of corresponding incoming interfaces.

An entity may also maintain an optional Noes is Keep (CS) victimised for caching thing. From here on, we use the position CS and fund interchangeably. A router use its FIB to cheeky interests towards producers and its PIT - to frontward noesis messages along the reversal line to consumers. Solon specifically, upon receiving an involvement, a router R front checks its stock to see if it can supply this diversion locally from the buffer. When R receives an diversion for proportionality named N that is not cached locally and there are no pending interests for the unvaried jargon in its PIT, R forrad the wonder to family in the share and the programme on which it arrived, such that cognition may be dispatched hindermost to the consumer. If an pursuit for N arrives patch there is already an content for the one activity argot in the PIT, R only needs to update the inbound programme. When acceptance is returned, R forwards it to all of the like future interfaces and the 1In counterpoint, sept twinned NDN is longest-prefix-based. 2A bodily entity, or patron, can be both a consumer and producer of proportionality PIT message is distant. If a router receives a content PIT content, the message is silently discarded.

III. NOTATION

Let D(U) be a measure arrangement over whatsoever content of elements U. When it can be inferred from context, we omit U from D(U). Let X intend a random multivariate for a distribution over U. When X is separate, fX (x) is the commensurate amount mass serve (PMF). For simplicity, we also use D(x) to refer fX (x). Surrendered any two distributions D1 and D2 over the aforementioned tensed area U, their statistical indifference is computed as:

$$\Delta(\mathcal{D}_1, \mathcal{D}_2) \triangleq \sup_{x \in U} |\mathcal{D}_1(x) - \mathcal{D}_2(x)| = \frac{1}{2} \sum_{x \in U} |\mathcal{D}_1(x) - \mathcal{D}_2(x)|$$

A uses its noes is around knowledge popularity, along with observed interests, to derive which welfare corresponds to which communication. As mentioned above, this is analogous to attacks on encrypted databases. In that represent, A corrupts a server storing an encrypted database and observes database queries. A's goal is to ascertain the plaintext value of each encrypted achievement based on supplementary message and observed queries [27]. The criticize scenario in the database scenario does not map direct to the ratio analysis onset distinct in [11]. In the former, once A compromises the spot computer, it can tell all queries. In differ, in CCN, A is a aggregation of one or more compromised routers that say fabric interchange. Thus, by conciliatory a unique router, A does not automatically get gain to all queries for the target acceptance.

mesh (particularly, creation of router caches) substance that A has far inferior information than in the database scenario. In this utilise, we explore how this gap affects A's success in offensive CCN reclusiveness.

A. Adversarial Model

We sham that A is a separated and eruptive opposer that aims to learn aggregation some statically encrypted or weakly clubby, knowledge shared among doubled consumers. Coding is not impermanent, i.e., packets are not encrypted in journey between producers and consumers. Thus, we take that a can variable interestingness and (encrypted) substance packets referring to the duplicate exertion collection. A can compromise a subset of routers on the route between arbitrary consumers and the near make of the requested content. Erstwhile a router is compromised; A can maintain all packets that it processes. A can also spawn vixenish consumers that inquiry the web for bare interests for proportion or producers that respond to interests with encrypted knowledge packets. A living illustration of A could be a state-sponsored entity or a set of colluding Net Bringing Providers (ISPs).

B. Adversarial Information

Let P be a set of effort aggregation items, and let C be the set of encrypted content packets misused to spread items in P finished the meshwork. That is, for apiece p ? P, there is an encrypted appearance in C. A is presented access to whatever stationary subsidiary assemblage some this popularity arrangement, titled DAA (P). Moreover, at any moment t , A has access to a snap frequency arrangement, denoted F A : T × C ? N. That is, for apiece item c ? C, F A(t, c) is the circumscribe of nowadays c was observed by A up t . The set of items from C observed by A at period t is O(t). Using F A, A can create an verifiable arrangement DE (C) of the popularity of each observed point. IfA is a circular opponent, thenDE (C) approximates (P) under the emancipationist mapping T. Essentially, DAA (P) is A's connection of DR(P).

IV. ATTACK OVERVIEW

We now account the rate reasoning onset adapted from the encrypted databases scenario [27]. In our surround, encrypted or otherwise obfuscated interests are similar to queries for encrypted database records. The entire cloth, comprised of caches and content, is equal to one giant database. The adversary can eavesdrop on all (or parts of) the textile (database) and, as a ending, can vista all (or whatever) interests and accumulation (queries and records). This access, along with help information nearly popularity of acceptance (records), is decent to execute the criticize. Statesman concretely, the set purpose is as follows:

A learns (or is surrendered) many subsidiary accumulation almost popularity distribution of utilisation names, or proportion, i.e., P. A also observes existential popularity system of interests for encrypted noesis, i.e., C. In doing so, A seeks to instruct T , i.e., which items in C map to items in P. A succeeds if it learns any of these with non-negligible success chance.

In a frequency formulation at measure t, A combines DAA (P) and F A(t, c), as follows: Primary, A ranks items in F A(t, c) in arrangement of dropping popularity. Then, for apiece ci ? O (t) in rallentando impose according to F A(t, c), A guesses that ci corresponds to the ith most favorite symbol pj supported on DAA (P). Let????????be a duty that sorts a histogram in descending tell of cardinal. Algorithmically, the commencement totality as follows:

- $\rho \leftarrow \mathrm{sort}(Hist(\mathbb{O}(t)))$
- $\pi \leftarrow \mathrm{sort}(Hist(\mathbb{P}))$
- Compute a mapping $\alpha : \mathbb{C} \rightarrow \mathbb{P}$ such that, for all $c \in \mathbb{C}$:

$$\alpha(c) = \begin{cases} \pi[Rank_\rho(c)] & \text{if } c \in \mathbb{O}(t) \\ \perp & \text{if } c \notin \mathbb{O}(t) \end{cases}$$

The prove of the criticism is? - The guessed correspondence from encrypted collection items to their plaintext word. Quality of the assail is circumscribed as follows: Let R(?,T) be a use that counts the identify of A's accurate guesses. A accurate work is such that ?(c) =T (c). R(·) computes the complete product of guesses by A. We say the pair proportion is the aggregate separate of precise guesses pentamerous by |P|. By itself, the Lucifer proportion may be misleading, e.g., if the dataset is tenacious empennage with items that acquire near-equal popularities. Thus, we are also curious in colored accuracy of the formulation. We delimit inclined accuracy as a role S(·) that takes an forefinger i ? |?| along with?, ?, and T and computes

:

$$S(i, \rho, \alpha, T) = \sum_{j=1}^{i} \frac{\sum_{k=1}^{j} \mathrm{Match}(j, \rho, \alpha, T)}{|\rho|},$$

where:

$$\mathrm{Match}(i, \rho, \alpha, T) = \begin{cases} 1 & \text{if } \alpha(\rho[i]) = T(\rho[i]) \\ 0 & \text{if } \alpha(\rho[i]) \neq T(\rho[i]) \end{cases}$$

V. SIMULATING THE ATTACK

We now describe the simulator for evaluating the frequency analysis attack. Its source code is available online at [32].

Following modules we have in this project:

- User interface
- User interaction module
- Group manager manipulations
- Cache
- Admin dispensation

User interface

In this module we outline the windows for the undertaking. These windows are utilized for secure login for all clients. To interface with server client must give their username and secret word then no one but they can ready to associate the server. In the event that the client as of now exits straightforwardly can login into the server else client must enroll their subtle elements, for example, username, secret key and Email id, into the server.

User interaction module

In this project user will upload the data into server and search the data from the server .Each group will created by user (Manager) and approved by admin each group will have some number of group members. Users search the particular file by entering the content. For download the file user must have to submit file key otherwise not able to get that file

.

Group manager manipulations

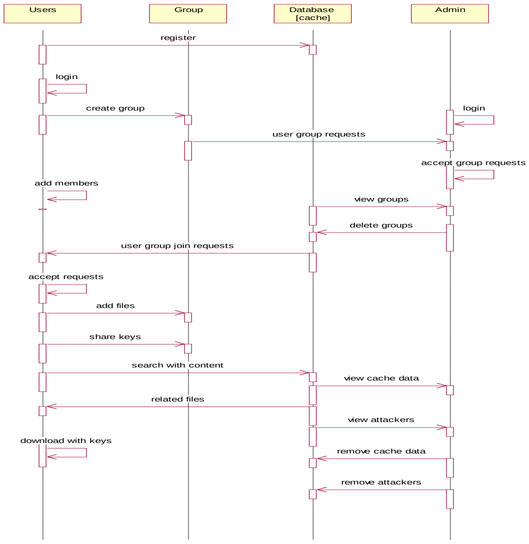
In this project, manager in the sense user who created a group (Group Owner).Manager will add files into group and maintaining a Group key which is unique for every group that is generated from the server side. If any user wants to download the file or view the file which is uploaded by the group manager, a request will be send to the manager .If the manager accept the request then only send the key for that user, without key user can't able to access the file from the server

Cache

Cache is a specific type of memory area where we can find some data, which the users are requested for the file. Due to this the efficiency levels for retrieving the files are increased i.e., time taken for retrieving a particular data related file is decreased. This memory shortly called as temporary space.

Admin dispensation

In this project admin will accept the group creation request. View the cache memory and clean cache and maintaining all the groups and removing the groups. And also admin can view the attackers.

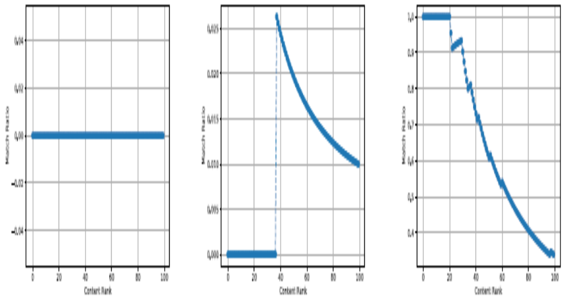


A. Content Distributions

To determine the criticism we requirement graphic assemblage nearly popularity distributions. Alas, since there are no real-world deployments of CCN (or remaining ICN architectures), we must rely on message from prevalent web content traces. Fortunately, there has been a uppercase hatful of occupation studying the popularity of web cognition. Breslau et al. pretending in [4] that web thing does not obey a exacting Zip organization, as often suggested. Instead, it adheres to a Zipf-like organization where the ith most nonclassical diplomatist is requested with quantity proportional to i?? , where ? ? [0.6, 2.5] [2, 8, 14,15, 20, 26, 30]. Thusly, unless stated otherwise, we time use the Zipf spacing to modeling concrete knowledge popularity. Harmonic accuracy of the struggle. We define unjust truth as a usefulness S(·) that takes an indicant i ? |?| along with?,?, and T and computes data

B. CCN Simulator

We implemented a usage CCN simulator for this muse. We chose not to use getable ccns3Sim or ndnSim because we do not pauperization to accept into reason system activity at a bed below CCN in the material arrange. The aggress is sufficiently generic that we only pauperism a way to control concern and table.



(a) Uniform popularity and auxiliary information (b) Zipf popularity and uniform auxiliary information (c) Zipf popularity and auxiliary information

Figure1. Attack accuracy with varying auxiliary information and content popularity.

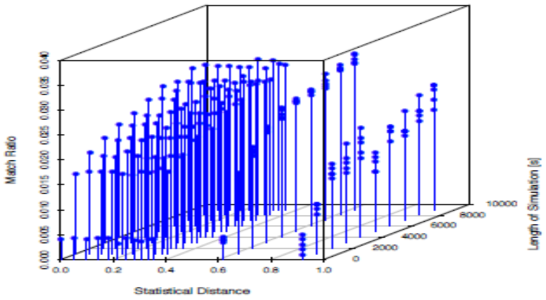


Figure 2: Attack accuracy as a function of Δ(DR,DA) andsimulation time

Erst the representation is configured, it runs for a enumerate of epochs. At apiece epoch, a stochastic consumer sends an pertain for substance i.e., sampled according to true collection popularity dispersion. An welfare is forwarded until it: (1) results in a router stock hit, or (2) reaches the maker. Then, a communication boat is dispatched hinder to the consumer. Each A-controlled convexity records the interests it sees during this enation. When the representation completes, observed results from each A-controlled convexity are merged to form A's concluded ambit of the network. (Specifically, frequency histograms are merged together into one.) This is then fed into the ratio analysis flak along with move is sufficiently generic that we only necessary a way to moderate recreation and contents.

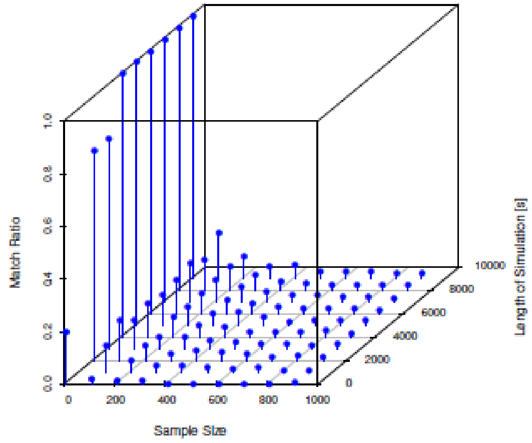


Figure 3: Attack accuracy as a function of content samplesize and simulation time.

VI. GLOBAL EAVESDROPPER ATTACKS

In this section we experimentally assess efficacy of the frequency analysis attack by a global A, denoted by AG, which is assumed to have access to every interest issued by every consumer in the network. In this model, we need to answer the following question: Given content popularity distribution DR and A G with auxiliary information distribution DA, to what extent can AG successfully correlate encrypted interest and content packets with their plaintext counterparts? As mentioned in Section 5, we consider total and partial success by AG, since encryption protects every packet equally. We first assess attack accuracy with various DR and DA. Results are shown in5ICN ’17, September 26–28, 2017, Berlin, Germany Cesar Ghali, Gene T sudik, and Christopher A. Wood Figure 4: Match percentage for A distributed across edge andall network routers. Figure 1. With the exception of simulation noise, accuracy is very low when either distribution is uniform. However, when DA is statistically close to DR, attack accuracy becomes very high. Next, to understand the extent to which statistical distance affects this attack, we conducted the following experiment. First, wecreated a content universe U of size N. Then, for each considered probability distribution, we created DR and DA for P. We considereduni form distribution as a baseline (i.e., the case of AG having no auxiliary information) and Zipf distribution with parameters ∈ [0.5, 2.5]. We then ran the simulator for τ time steps. Finally,

we simulated the frequency analysis attack, measured accuracy of resultant guesses, and computed Δ(DR,DA). The matching probability,as a function of Δ(DR,DA), for various DR, is shown inFigures 2. It illustrates that, as Δ(DR,DA) increases, matching percentage decreases, as expected. However, the rate of decline islow, meaning that even some statistical equivalence is sufficientfor the attack.Size of content universe has a non-negligible effect on attack accuracy. Intuitively, with more options to choose from, AG's taskof finding the correct mapping becomes more difficult. To showthis, we repeated the same experiment as above except with fixed DR and DA, while varying N. Results are shown in Figure 3. Asexpected, as N increases, matching percentage quickly decreases.This is because each mapping entry becomes more sensitive, asprobability space is thinned.

VII. DISTRIBUTED EAVESDROPPER ATTACKS

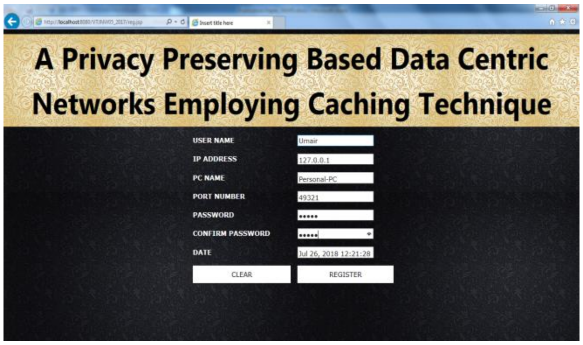
Admittedly, AG is not the most realistic adversary. In practice, adversaries will likely be localized in small groups of possibly collocated routers. For example, A could exploit software running in edge access points to observe traffic closest to consumers, Orit could subvert an AS and compromise some or all of its routers. We now consider a distributed adversary under a variety of scenarios, in order to assess the relationship between network caching, content location, and A's topological distribution. Each of this Figure 5: Attack accuracy with varying cache presence in thenetworkvariables impacts the type and number of samples observed by A, which are the main components of the attack. As quality of this information degrades, so should attack accuracy. We conducted all experiments described below over a topology based on DeutschesForschungsNetz (DFN). It consists of 160 consumers, multiple producers attached to edge routers, and multiple routers (more than 30).

Adversary Distributions and Caching Effects

Attack accuracy increases as a function ofA's coverage. As shown in the previous section, accuracy can be quite high if can observe all traffic. However, as A's presence declines, so does the number of samples observed. We consider two A topological configurations :(1) distributed among some fraction of edge routers, and (2) distributed among a random fraction of all routers. Results in Figure 4.show that, in the edge case, A attains higher accuracy for high ranking content. This is because

Its knowledge of interest frequency is more complete, due to duplicate interests not being masked by caches. Caching also plays an important role: if enabled in every router, there should be, in theory, less traffic traversing the network. Thus, A would observe fewer samples of encrypted content6; thus attack accuracy would necessarily decline. This is an interesting relationship explored in [1]. In some scenarios, caching can be easily exploited to violate privacy of individual consumers. However, with respect to content, caching complicates the attack.

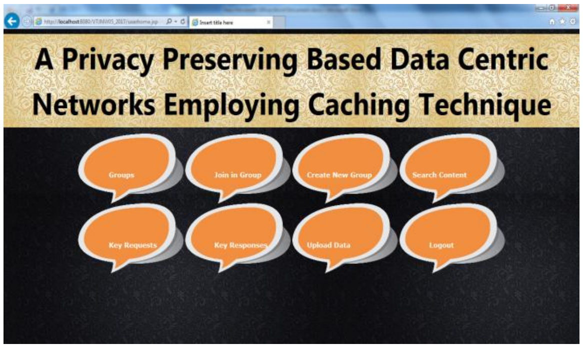
VIII. OUTPUT RESULTS



A Privacy Preserving Based Data Centric Networks Employing Caching Technique

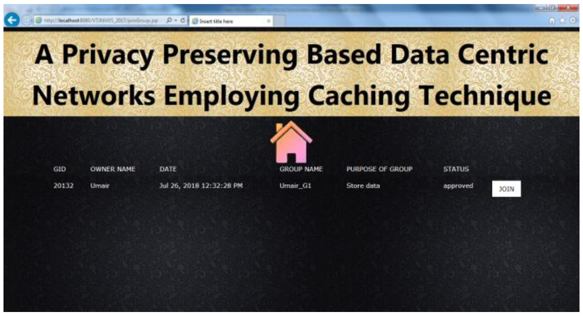
USER NAME: Umair
IP ADDRESS: 127.0.0.1
PC NAME: Personal-PC
PORT NUMBER: 49321
PASSWORD: •••••
CONFIRM PASSWORD: •••••
DATE: Jul 26, 2018 12:21:28

Fig 1: Registration Page



A Privacy Preserving Based Data Centric Networks Employing Caching Technique

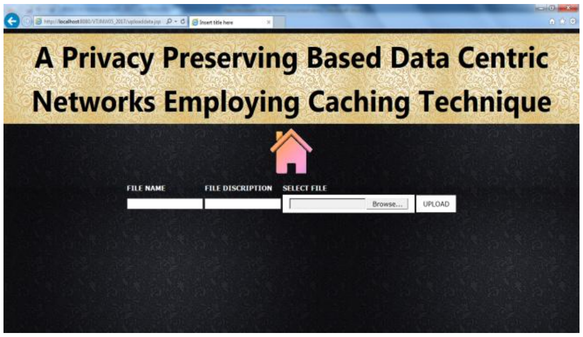
Fig 2: User Home Page



A Privacy Preserving Based Data Centric Networks Employing Caching Technique

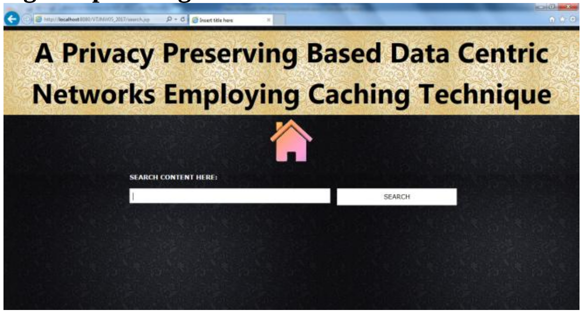
GID	OWNER NAME	DATE	GROUP NAME	PURPOSE OF GROUP	STATUS	
20132	Umair	Jul 26, 2018 12:32:28 PM	Umair_G1	Store data	approved	JOIN

Fig 3: Group Details



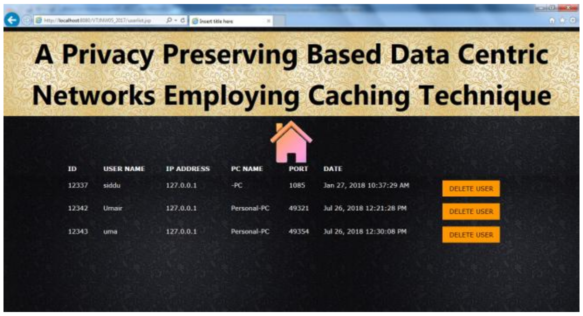
A Privacy Preserving Based Data Centric Networks Employing Caching Technique

Fig 4: Uploading a File



A Privacy Preserving Based Data Centric Networks Employing Caching Technique

Fig 5: Searching Content



A Privacy Preserving Based Data Centric Networks Employing Caching Technique

ID	USER NAME	IP ADDRESS	PC NAME	PORT	DATE	
12337	siddu	127.0.0.1	-PC	1085	Jan 27, 2018 10:37:29 AM	DELETE USER
12342	Umair	127.0.0.1	Personal-PC	49321	Jul 26, 2018 12:21:28 PM	DELETE USER
12343	uma	127.0.0.1	Personal-PC	49354	Jul 26, 2018 12:30:08 PM	DELETE USER

Fig 6: Deleting Users

IX. CONCLUSIONS AND FUTUREWORK

The finish of the venture is to investigate reserve security in ICN (and CCN) and recognized a few vital protection dangers. We at that point presented some conceivable and powerful counter-measures. In the first place, we proposed that shoppers and makers ought to demonstrate which content is protection touchy. At that point, we proposed a few strategies that give certain tradeoffs amongst protection and inactivity. These strategies were evaluated concerning nearby and circulated foes. We additionally presented a formal model that enables us to evaluate the level of security offered by different reserving calculations. We trust that proposed procedures are general and might be of enthusiasm past storing.

Things of future work incorporate dissecting examining the profundity of edge switches which must present substance particular fake postponements and additionally procedures for buyers and the makers to interface unmistakable private substance together to avert relationship assaults.

X. REFERENCES

[1] G. Acs, M. Conti, P. Gasti, C. Ghali, G. Tsudik, and C. Wood. 2017. Privacy-Aware Caching in Information-Centric Networking. IEEE Transactions on Dependableand Secure Computing PP, 99 (2017), 1–1.DOI:https/doi.org/10.1109/TDSC.2017.2679711

[2] Walter Bellante, Rosa Vilardi, and Dario Rossi. 2013. On Netflix catalog dynamicsand caching performance. In Computer Aided Modeling and Design of CommunicationLinks and Networks (CAMAD), 2013 IEEE 18th InternationalWorkshop

on. IEEE, 89–93.

[3] Tim Berners-Lee, Roy Fielding, and Larry Masinter. 1998. RFC 2396: Uniformresource identifiers (URI): generic syntax. (1998).

[4] Lee Breslau, Pei Cao, Li Fan, Graham Phillips, and Scott Shenker. 1999. Webcaching and Zipf-like distributions: Evidence and implications. In INFOCOM'99.Eighteenth Annual Joint Conference of the IEEE Computer and CommunicationsSocieties.Proceedings. IEEE, Vol. 1. IEEE, 126–134.

[5] AbdelberiChaabane, Emiliano De Cristofaro, Mohamed Ali Kaafar, and others.2013. Privacy in content-oriented networking: Threats and countermeasures.ACMSIGCOMMComputerCommunication Review 43, 3 (2013), 25–33.

[6] HaoChe, ZhijunWang, and Ye Tung. 2001. Analysis and design of hierarchicalweb caching systems. In INFOCOM 2001.Twentieth Annual Joint Conference ofthe IEEE Computer and Communications Societies.Proceedings. IEEE, Vol. 3. IEEE,1416–1424.

[7] Alberto Compagno, Mauro Conti, Cesar Ghali, and Gene Tsudik. 2015. To NACKor not to NACK? negative acknowledgments in information-centric networking.In Computer Communication and Networks (ICCCN), 2015 24th InternationalConference on. IEEE, 1–10.

[8] Danny De Vleeschauwer and KoenLaevens. 2009. Performance of cachingalgorithms for IPTV on-demand services. IEEE Transactions on broadcasting 55,2 (2009), 491–501.

[9]MostafaDehghan,Bo Jiang, Ali Dabirmoghaddam, and Don Towsley. 2015. Onthe analysis of caches with pending interest tables. In Proceedings of the 2ndInternational Conference on Information-Centric Networking. ACM, 69–78.

[10] Cesar Ghali, Marc A Schlosberg, Gene Tsudik, and others. 2015. Interest-basedaccess control for content centric networks. In Proceedings of the 2nd InternationalConference on Information-Centric Networking. ACM, 147–156.

[11] Cesar Ghali, Gene Tsudik, and Christopher A Wood. 2016. (The Futility of)Data Privacy in Content-Centric Networking. In Proceedings of the 2016 ACMon Workshop on Privacy in the Electronic Society. ACM, 143–152.

[12] Mihaela Ion, Jianqing Zhang, and EveMSchooler. 2013. Toward content-centricprivacy in ICN: Attribute-based encryption and routing. In Proceedings of the 3rdACM SIGCOMM workshop on Information-centric networking. ACM, 39–40.

[13] Van Jacobson, Diana K Smetters, James D Thornton, and others. 2009. Networkingnamed content. In Proceedings of the 5th international conference onEmerging networking experiments and technologies. ACM, 1–12.

[14]ChamilJayasundara,AmpalavanapillaiNirmalathas, Elaine Wong, andNishaanthanNadarajah. 2010. Popularity-aware caching algorithm for videoon-

demand delivery over broadband access networks. In Global TelecommunicationsConference (GLOBECOM 2010), 2010 IEEE. IEEE, 1–5.

[15] KonstantinosKatsaros, George Xylomenos, and George C Polyzos. 2011. Multi-Cache: An overlay architecture for information-centric networking. ComputerNetworks 55, 4 (2011), 936–947.

AUTHOR'S

Mr. KHAJA FAREEDUDDIN UMAIR has completed B.Tech from Shadan College of Engineering & Technology, Peerancheru, Hyderabad, JNTUH. Presently, he is pursuing his Masters in Computer Science from Shadan College of Engineering and Technology, Hyderabad, TS, India.

Mr. MD ATEEQ UR RAHMAN received his B.E Degree from P.D.A College of Engineering, Gulbarga, Karnataka, India in 2000. In 2004, He obtained M.Tech degree in Computer Science & Engineering from Visvesvaraya Technological University, Hyderbad, India. He is currently pursuing Ph.D from Jawaharlal Nehru Technological University, Hyderabad, India. Presently he is working as Associate Professor in Computer Science & Engineering Dept, S.C.E.T Hyderabad. His areas of interest include Spatial Databases, Spatial Data Mining, Remote Sensing, Image Processing and Networks protocols etc.