 doi:10.20944/preprints202105.0179.v2

Article

DSAC-Digital Signature for Access Control in Information Centric Network

Zaki Ullah [1,†,‡], Muhammad Inam Ul Haq [2,†,‡], Samiullah Khan [3,†,‡], Muhammad Zubair [4,†,‡]

[1] Khushal Khan Khattak Univerity Karak 1; zakiktk99@gmail.com
[2] Khushal Khan Khattak Univerity Karak 1; muhammad.inamulhaq@kkkuk.edu.pk
[3] The University of Agriculture Peshawar 2; samikhan.1982@gmail.com
[4] Khushal Khan Khattak Univerity Karak 1; dr.muhammadzubair@kkkuk.edu.pk
* Correspondence:samikhan.1982@gmail.com ;) +92-0333-940-0232 (F.L.)
† Current address: The University of Agriculture Peshawar
‡ These authors contributed equally to this work.

Abstract: The world is growing very rapidly concerning technology. In the next-generation Internet, the existing architecture requires to be upgraded from Host-Centric Networking paradigm to Information-centric networking architecture. The unique aspect of information-centric networking is in-network cashing. Due to the system augmentation and In-network cashing technique, this novel system needs extremely high content security to ensure system integrity and maintenance. 5G network may be supported by the Information-Centric Network due to its high data transmission rate. In order to handle the serious security issues such as attack on confidentiality, authentication and integrity of the content, a Digital Signature based Access Control Mechanism in Information-Centric Network (DSAC) scheme is proposed to enhance security of ICN. Briefly, this new scheme uses Digital Signature, hash function, Trusted Third Party (TTP) and Proxy TTP. The client request for content, after receiving a request, the content provider generates and encrypts content with the digital signature and random value 'k' hash function and send it to TTP. After the signing process, the TTP sends the encryption hash key to Proxy TTP. In this proposed scheme authentication, confidentiality, the integrity aspects of the content security are improved.

Keywords: Access control; Digital Signature; Trusted Third Party (TTP); Proxy TTP; Information-Centric.)

1. Introduction

The Internet is a phenomenon of interconnected networks formed in the early 1960s with the main aim to connect computers and share resources like data and devices among the research community. In the last few decades, the Internet has significantly advanced and has become the most important mean of communication among the users and devices to ensure global access to many services as well as information in a convenient way. The Internet has exhibited great success since its inception by globally connecting billions of heterogeneous devices, by providing services and knowledge [1]. With the advancement in technology, Internet communication moved to content-based interaction instead of point-to-point communication. The content might be file sharing, web pages and video retrieving. The content consumer primarily focuses on the accessibility, authenticity and integrity of the content itself, instead of concerning about location where the content resides. The concept of content-based interaction is achieved by recently suggested different architectures of Information-Centric Network (ICN)[2].

Information-centric network (ICN) is a novel networking architecture in which contents will be used as objects. ICN is entirely based on content i.e. client requests for content by its name. In ICN routers can store content, for a limited time, for future use and the content when asked for by explicit request using its name is called interest. The ICN routes the interest either from the content producer or from the router that it has stored. Now if there is a request for certain interest, it will instantly be provided to the

 doi:10.20944/preprints202105.0179.v2

requesting client. In ICN routers also stores the path of requested interest, from a client, so that it can channelize the content back to the destination[3]. The main objective of ICN architecture is to provide information to each customer easily. In these networks, data and information are considered as objects which lessen the role of hosts in comparison to the other networks. Moreover, the end-users are not interested in the location of the content rather in the contents to be accessed through its name, thus the ICN causes to change the nature of the modern internet architecture[4].

The existing Internet architecture is going to have a paradigm shift from hosts based networks to the Internet of things, media-based internet, mobile-based Internet and masses based Internet. Thus it requires highly flexible and well-organized contents allocation, which can be fulfilled by the ICN. The ICN can arrange the amount of interest, higher than the number of customers in the present internet architectures. It is predicted that by 2020, around 26.3 billion internet devices would be connected globally, normal broadband speed will become 47.7 Mbps, the number of internet users will be 4.1 billion and IP video traffic would become 82% of the total network traffic[] [5]. While a huge part of network traffic is file sharing, particularly video sharing, different ICN architectures like content centric network (CCN), name data network (NDN), Network Information (NetInf), Data-oriented Network Architecture DONA are proposed. ICN architecture is meant for moving client-server connections to consumer-content connections, thus the concern of the network changes to legitimate content copy from the content owners address identification. As a result, the clients don't want to know the location from where the content comes, i.e. the IP address of the content owner, thus the content name is enough to provide the content copy to the client. Content owners publish the contents which can be copied and cashed in the network using network cache. This arrangement enables content being efficiently provided to the consumers[5].

So, the basic idea behind ICN architectures is that the required information is more important in comparison to the person who is communicating contrary to the present host-centric network in which importance is given to person than the required information. To alleviate the present day internet congestion, ICN can be proved more helpful by sharing contents and local ICN router is allowed to cash the information locally. In ICN, the IP bundle is to be replaced by name-based content therefore IP would no more be of use in future. In ICN, the information is more significations as compared to the hardware in the current architecture. Furthermore, by accepting name-based content's obvious confirmation, ICN gives importance and priority to locally available content which is the only aspect of ICN (in-network caching). However smartly basic, recognizing ICN as an overlay on the present Network prompts an irrational extended multifaceted nature of IP directing; hence it is difficult to manhandle ICN value in inheritance network[6].

With the advancement in technology, the Internet has observed a paradigm shift the concept of the host has expended, ranging from the conventional workstations to services, people, media and things(like home appliances, vehicles etc). Thus at present, we have Internet of people, Internet of services, Internet of things, equipped with very fast, flexible and well-organized content allocation mechanism. ICN plays a vital role in implementing this advanced Internet paradigm, for which several architectures have been proposed like; Named Data Networking (NDN), Public Subscribe internet technology (PURSUIT), Data Oriented Networking Architecture (DONA), and Network if Information (NetInf). All these architectures share a few common features i.e. security, application programming interface, caching, routing, information object, and naming etc[7]. Contents have two categories in ICN, i.e. restricted access content and open access content. The conventional access control scheme is not applicable over the ICN because of the three features given as in-network caching, ICN does not depend on IP addresses, and ICN interest has no user

 doi:10.20944/preprints202105.0179.v2

identification information[8].

The ICN architecture decouples location and identity, thus supports consumers mobility. Similarly, due to time and space decoupling in ICN architecture, the content providers (CP) and consumers do not require to know each other's locations as well as online time. The key characteristic of ICN is content caching or in-network caching, which permits nodes to cache any content to enable a consumer to retrieve content from different locations and this technique makes the access control in ICN is more complex. In-network caching boosts data availability by decreasing network load and response time but at the same time, it raises security concerns for the ICN because only authorized user should be allowed to access the cached contents. Since decryption information is needed to access different data items in ICN making data security more significant. Several security models have been proposed in ICN in about its different feature in which content security is given priority instead of the transmission channel. Moreover, data integrity and authenticity in ICN is ensured by the digital signature of the data packages. It is very much clear that the ICN is much secure as compared to traditional networks, however unauthorized content access, collusion attack and content analysis could happen from intruders. Access control in ICN is applied in such a manner that legitimate users can access specific content while illegal users can't[9].

1.1. In-Networking Caching

In-network content caching is an advanced and salient aspect of ICN, which has not been used before in any network. In ICN the content is fetched by its name and every router is outfitted with a segment of storage for storing the copy of contents passing through it. This cached copy is then used to fulfil the future interest request regarding the same cached content. The intermediate router provides content packets to the clients without letting the client know the sender location, whether the content has come from the server or the middle cache router[10]. In-networking caching is best in the sense of energy efficiency. Due to in-network caching the energy consumption is reduced as the delivery distance is reduced. Because of the limited storage capacity of the router, it is necessary to decide which content is best to store, where to store, for how long it should be stored and how to throw out a cached content to allow a new one. The storage in the router is known as the content store (CS)[11]. ICN router also stores the requested content path; the content sent by the server is forwarded back to the client on the way as requested by the client. Each router has a pending interest table (PIT) used to store the content request which is not satisfied yet. This In-network caching technique has various advantages i.e. it is more scalable, easy to implement, and friendly for both content client and content producer[12].

1.1.1. Caching

Content Caching is one of the inimitable aspects of ICN, in which every intermediate router is outfitted with a small amount of memory to cache the content for the future. The cached content shall be locally served to the interest with comparatively less delay. ICN is a decentralized storage model because routers are located in a distributed manner in the network where legitimate customer can access any content from any router needless to have permission from the content producer. Also, due to in-network caching the ICN guarantees congestion control, lessening the load on the server, reduce delay with smaller transmission path, and minimize computational overhead. In-network caching can raise serious security concerns like cache snooping where caches are probed to determine the presence of content. For instance, an illegitimate user may find out a content being demanded by its neighbours or some producer has recently forwarded a piece of content. An Encryption process is proposed for content security, to immune content from unauthorized user access because conventional content security, confidentiality and authenticity, is not

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2021 doi:10.20944/preprints202105.0179.v2

enough.[13][14][15].

In-networking content caching is extremely efficient for energy conservation. A very small amount of energy is required to access content from a near-by router in comparison to its access from the original producer as the delivery distance is reduced. ICN uses Caching Everything Everywhere (CEE) mechanism by default, means every node in the forwarding path can take a copy of the passing content to manage the Least Recently Used (LRU) replacement strategy. However, if the interest generated for the same content that will be willingly satisfied by the first cached router and minimum resources will be used for this. But the content caching memory in ICN router is too restricted and a good and useful decision is to be taken that which content is more necessary and qualified for storage, and how long the content should be cached when some new content is necessary to be cached[16].

The following method is used for content caching and forwarding[17].

1. Pending Interest Table (PIT)
   ICN routers keep unfulfilled interests in PIT. If a node generates some interest, the router searches its cache to serve the interest. If the match is found, the content is provided to the consumer; otherwise, the router checks its PIT to check the already exiting interest for the same content. In case, PIT has already an interest stored for the same content, the coming one is added with it and is forwarded to the next router according to FIB table.
2. Interest Base (FIB) Table
   ICN routers through this table decide that the arriving packet should be forwarded to which next node. It is used to rout the interest towards the consumer of the requested content by using prefixes with the forwarding content name according to their long-prefix-matching (LPM).
3. Content Store (CS)
   Content store caches content copy. CS specifies a time frame for how long should the content be stored and after expiry time the content should be drafted out from the CS.

1.1.2. Caching update

The difference between the IoT and the conventional Internet is content creation. In the conventional Internet, content is created by humans and kept on servers for a long duration. On the other hand, it is generated by devices in the IoT network. These contents are small, created for a short time, and are updated regularly. They are also referred to as transient content[18]. IoT nodes usually have fresh and updated contents; therefore, an efficient cache update method is required. The most prominent cache update strategy in the literature is described in, which is based on the content freshness. In this strategy, a freshness factor is used that decides the update time for particular cached content. This strategy keeps the IoT cache updated by evicting the old and outdated contents. Similarly, an event-based freshness mechanism is proposed, where the expiration time is used to know how long content has stayed in the cache[19][20].

1.2. Access Control in ICN

The significant characteristic of ICN is to ensure secure access control (AC) enforcement mechanisms i.e. content sending and receiving through their names. Due to in-network content caching, access control is more crucial. When a client desires to access content, it just sends the name and the relevant Id, encrypted by its public key. To fulfil the request, the controller verifies the authenticity of the client. When the client is found legitimate then checks the client approval to get the content before sending information. Here the client's revocation occurs. After all these steps the content is dispersed in the network. Once the content spread over the network it may be stored inside each router to fulfil the future demands for the same content locally without checking the user's identity.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2021 doi:10.20944/preprints202105.0179.v2

This means after spreading the content, the content provider loses control over the access of content that who gets the content[21].

1.3. Cryptography

Cryptography is the technique of hiding the original message/information from eavesdropper that can only be accessed to authorized users. It is normally used for ensuring the privacy and secrecy of the transmitted data over an unsecured channel and prevent eavesdropping and data tampering[22].

Cryptography has the following main characteristics.

1. Confidentiality
   It means that no unauthorized user can read the secret information.
2. Authentication
   The producer and subscriber can check each other identity for communication.
3. Integrity
   Integrity means that the content cannot be changed during storage or while forwarding from sender to receiver.
4. Non-repudiation
   If a sender or provider of content can deny creation or transmission of their transmitted content later, non-repudiation can occur.

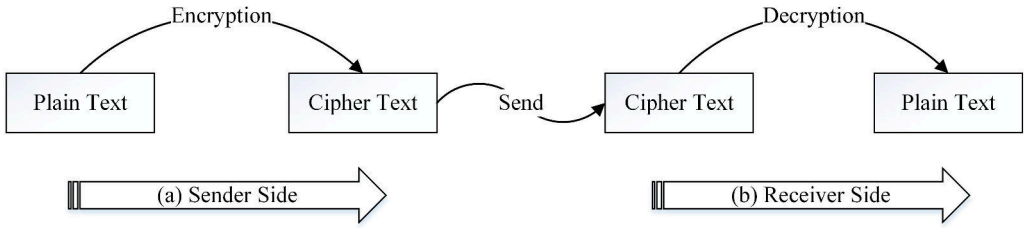

Figure 1. Content encryption procedure .

1.4. Digital Signature

The digital signature is a mathematical scheme used to verify the authenticity and non-repudiation, of a digital document or message, which allows the sender of the message to attach code as a digital signature. It is used, when determining authenticity and avoiding tampering are important, like financial transactions. Normally, a digital signature is produced by retrieving the hash function of a message called 'message digest'. The digital signature also guarantees the source and integrity of the message. The first ever approach revealed for digital signature was 'Rivest-Shamir-Adleman (RSA)' digital signature technique which remains one of the most important and adaptable mechanisms in today's networks for security issues [23].

Digital signatures authenticate electronic documents in much the same way as the handwritten signatures authenticate printed documents. Recipients of electronic documents accompanied by digital signatures may verify that senders are whom they claim to be and that the documents have not been altered from the time of transmission. In other words, senders may not disown digital signatures by claiming that they have been forged, and recipients can verify the identity of senders as well as the integrity of the documents[24].

1.4.1. Blind Digital Signature

The blind digital signature is an extension of a digital signature. It has gained much important due to the widespread use of e-payment, e-banking and e-voting system. It is also used for security, privacy and identity of the client in anonymity preserved communication. Mostly current internet users prefer to have anonymous interaction system to

immune their identity from other connected clients. Thus blind Signcryption is mostly used for sharing sensitive information and for the devices with low processing as well as the small size of memory like smart phones etc. It also has the following essential characteristics which are very necessary for today network. i.e. integrity, confidentiality, authenticity, anonymity, unforgeability, unlink-ability, blindness, and intractability with efficiency in computational and communication overhead[25].

To enhance the security of ICN content, a Digital Signature Access Control (DSAC) scheme is proposed. In this scheme, the client requests for content encrypted with their private key and send to the content producer through edge router then through ICN. The content producer generates the requested content encrypt it with RSA based digital signature and sends it to Trusted Third Party (TTP) to encrypt the content using hash value 'k'. The TTP sends the ciphered content to the requesting user through ICN. Each router in ICN can cache the content copy and forward it to the next node until the content reaches the destination node. At the destination node, the content is decrypted with the already shared public key and a hash value of 'k'. TTP uses the Digital Signature cryptography technique for the confidentiality, authentication and integrity of data. Proxy TTP is used to check consumer authentication locally. This research mainly focuses on confidentiality, authentication and integrity of data in ICN.

1.5. Statement of the Problem

Information Centric Network also known as Future Network or Next Generation Internet is necessary to develop support for the coming very high speed 5G network. In 5G network, the data rate is very high which is very difficult for the present host-centric network to support. Access control in ICN has been one of the hard topics of research for many years, to secure the contents shared on the network. In ICN, information is more important than the hardware operating on it. Other access control protocols in ICN such as Decentralized Access Control Protocol for ICN (DACPI) protocol and Decentralized Elliptic curve-based access control (ECAC) protocol faces delay, need of extra storage space and heavy computational overhead. The research work performed a batter scheme for ICN content security, to augment the content security and easily available to all legitimate users. A Digital Signature Access Control for Access Control in ICN (DSAC) scheme is proposed to improve the security of the content. Trusted Third Party (TTP) and proxy TTP will also be involved in this ICN architecture to make the content secured and integrated. Authentication, Confidentiality and integrity of data and authentication of consumer problems shell remain the main focus in this research work.

1.6. Significance of the Study

This study would be useful for: i. To improves security for ICN contents. ii. To secure the decryption key from the network channel/ to change the decryption key out from content distribution way. iii. To increase confidentiality/integrity of the content by using the Trust Third Party and Proxy trusted the third party. iv. For content Security Digital signature and Hash function (SHA-256) are used.

1.7. Limitations of the Study

The proposed access control security mechanism provides authentication, confidentiality and integrity using public key cryptography (RSA), digital signature (SHA-256) and a random generated Nonce for content security. The novelty of this scheme is to generate a new security key after first access by any proxy TTP within the region for a new user. Someone can also implement the same technique (ECC) for any smart IoT based network, which can support high bandwidth channel for communication. Information centric networking is the only architecture that supports 5G technology due to which the smart city project can easily be implemented in the world.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2021 doi:10.20944/preprints202105.0179.v2

1.8. Aims and Objectives

The major objectives of this research work are: i. To proposed a scheme that will provide authentication, confidentiality and integrity of data in ICN. ii. To use the TTP and proxy TTP for authentication of the consumer.

2. Related Work

In this portion, the focus is on the literature study of secure access control in ICN and their limitation for future work to enhance the security and privacy issues of contents in information centric network. The researcher in the space has as of late begun investigating these issues.

E. G. AbdAllah et al [26] use Elliptic curve-based access control protocol has been used for content security in information centric network. When subscriber requests for content, the requesting message is encrypted by producer public key and random positive integer 'k2'.The value of 'k2' is not known to anyone except subscriber. The requested interest also has the nonce value 'n2'. On producer end, to extract the nonce 'n2' value, the producer decrypts the message by own private key not know the value of k2. Now the publisher sends another message encrypted with subscriber public key and random value 'k1', which will not be known to anyone except publisher. The message also contains two nonce values 'n2 and n1', Elliptic curve parameter, the public key of publisher which is then used for the exchange of key. ICN network forwards the message to the subscriber. Now subscriber extracts the nonce value of n1 by using their private key to decrypt the message without knowing random number 'k1'as caption in Figure2. The subscriber also finds out the public parameter (Y) and secret key (S). The subscriber sends the message containing a hash value, public parameter 'y', the nonce value 'n1' and content name. At first, the edge router checks the authenticity of the user then sends the requested content to the subscriber. The transmitted contents are encrypted with shared key 'S' and subscriber public key, and finally, the content is accepted. The subscriber then checks the hash value received from the publisher and compares it with its hash value, if it matches, it means that the received content is original.

Limitation: - In this article, a lot of additional storage is required for storing the nonce values and public parameter on both sender and receiver side, heavy computation is required for such complex encryption and decryption, and also delaying occur in each content.

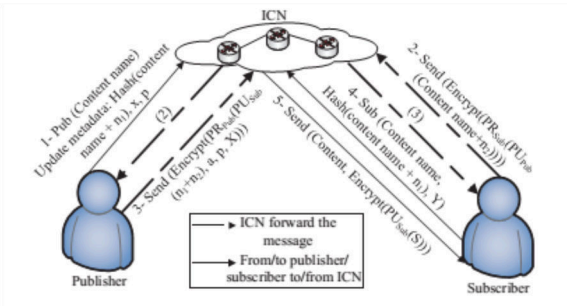

Figure 2. Decentralized access control protocol in ICN (ECAC) .

B. Li et al [5] proposed a model for conducting attribute based access control (ABAC) and attribute based encryption (ABE) through a Trusted Third Party (TTP). TTP is an independent node trusted by all the entities of the network. TTP also generate and manage global security parameter for the network. In this scheme, each client has a unique identifier 'UID' and a set of attributes. This 'UID' can also be used as an attribute. All the attributes other than 'UID' can be generated and allocated by any entity of a network and is known as the authority of the attribute. The attribute authority (AA) is semi trusted node that generates and manages a set of attributes shared in the network. When a content owner

 doi:10.20944/preprints202105.0179.v2

wants to broadcast the content, the owner determines which attribute will be used for content access control, which one used for content description and which one will be used for content search. Thus this attributes are distinguished by access control attributes 'ACA' and descriptive attribute 'DA'. After reaching content to network end-users only those users can decrypt the content that has the same attribute which is used for that content decryption. If attributes match the user can access that content otherwise content cannot be decrypted.

Limitation:-Client revocation remains a challenge mentioned in [21].

X. Tan et al [9] proposed a framework for access control in ICN. The framework deals with all types of digital files (like video, music and picture) as content. In this framework content publisher, CP registers users through a registration process and provides public and private keys to the registered users. The CP provides information about data decryption specific to each user as it is encrypted by the user's public key. The information thus generated is then attached as blocks to the blockchain and the CP releases new block to the whole network. Latest blockchain (decryption information) is provided to user and content is served to it, against its interest, by CP or an intermediate router. Content or data received from an intermediate router needs less time and low network congestion. The user can get its decryption information from the blockchain through its private key and can easily get original content. By using the blockchain technique only legitimate user can access the content, and it is very difficult to amend the content. With small changes, the data will be messy and helpless for content publisher management of authorized users.

Q. Li et al[27] proposes mandatory content access control procedure containing four labels 'h', 'n', 'd', 'p' used for the different security access level. Labels, 'h' denotes the highest protection level, 'n' is non-delegatability level, 'd' is delegatability level and 'p' is publically accessing level as shown in figure 3. The content publisher will send a content labeled with a certain label as shown in figure 2. The content with label 'h' cannot be stored in any ICN router, and shall only be forwarded to reach to destination end. While content with label 'n' can be stored only by the first router and then reclassify that label 'h' so that no one can store the content later. The content with label 'd' can be cached in more than one routers of the network. The content labeled 'p', can be read and cached by each router of the ICN network. Figure 2.2. Different ISPs can have different permissions to cache contents

Limitation: -Delay and router overhead can occur due to reclassification of the label[27].

Zheng et al. [28] consider an access control scheme in which the edge router performs content encryption. The publisher encrypts the content with its public key and a random key 'k1',to publish it on the network and cashed by the service edge router. The edge router selects a random secret key 'k2' to re-encryption the contents before sending it to the destination. For the decryption process, the client sends a content name, its identity and random key 'k2' to the publisher. The publisher checks client identity and access level and processes their private key along with 'k1'and 'k2'to create decryption key 'k' for a customer. When 'k' is received to a client it decrypts the received content. It may be noted that the decryption key 'k' will be separate for every content. Limitation: -In this paper due to the edge router re-encryption process it will take at least 10 seconds for even a very small content (256 MB). Due to the edge router encryption the resources used for encryption is undermines the scalability of the solution, because future internet is mostly loaded due to multimedia transmission/traffic [22].

Fotiou et al[29] discussed Identity Based Proxy Re-Encryption (IB-PRE) scheme for ICN. In identity based encryption, arbitrary strings are used as a public key. For content encryption, public key generator 'PKG' is used, by accepting secret key value 'k' to generate Master Secret Key 'MSK' and System Parameter 'SP', where the MSK is secret and SP is published publicly. In first encryption arbitrary string ID of a message, and SP is used to convert the plaintext to cipher text. This content will decrypt by using CID, the private key of the subscriber and get the plaintext message M. While during proxy re-encryption is

 doi:10.20944/preprints202105.0179.v2

a semi-trusted third party used to encrypt the cipher text; this encryption is performing through the public key of the client (delegator). This content will be decrypted by using client B (delegate) own secret private key.

Limitation: -Delay and Computational overhead occur due to two-time encryption [29].

S. Misra et al[30] proposed an AccConF mechanism for information centric network to secure the entire content transmission between content provider to intermediate in-network caching node and to end user. AccConF mostly focuses on the access to secured contents by legitimate users only. AccConF leverages broadcast encryption and especially targets mobile users. For content or group of content encryption, the content provider uses secure symmetric key encryption algorithm. A content or set of content may be encrypted using the same secret key, and only those authorized users can decrypt the content using the shared secret key. The content publisher can use different secret keys for the encryption of content or set of content. The author assumes the front-end player for the decryption of content, but the customer cannot store the symmetric key after decrypting the content. This framework uses a symmetric key and public key infrastructure.

Limitation: -if a single packet is damaged or does not reach safely to the destination the whole block is damaged [30].

S. Misra et al[31] Broadcast Encryptions (BE) technique was used for generating a symmetric key for the network. There are three steps used to encrypt and decrypt the content, the first server generates polynomial of degree 't', and calculate a number of points 'n' on it. The server then distributes the calculated points 'n' among the network nodes, and keeps polynomial 't' of them as its share. While in the second step the server generates some enabling blocks, containing secret symmetric key 't' which is then used to extract the secret key by end user, and then the enabling block is forwarded to the router in which the content is cached and forms an important part of the content. At last, the legitimate users can extract the embedded secret key from the received enabling block, and access the content. Limitation:-In paper [31] the cached content may read by the recently revoked user as the table may not be updated yet.

N. Fotiou et al [32] propose Attribute based and proxy base access control mechanism for Publish Subscriber Internet–Information Centric Network (PSI-ICN) architecture. In this mechanism a generalized rendezvous points are used, which perform a lookup for entire information, and these network nodes mediate content demand and supply to manage access control policies. This mechanism also proposes identity-based proxy re-encryption to immune content from the content publisher. The content will be encrypted independently due to their access control policies. The content will be recognized by two identifiers, the rendezvous identifier (RId) and scope identifier (SId). SIds are globally unique, and RIds are unique within a scope. SIds are used to give a "hint" about the network location of a content item. In particular, each Sid is managed by a lookup node known as the rendezvous node (RN). Where 'RN' manages a 'SId' as the rendezvous point (RV) of the SId. The 'RV' of a 'SId' maintains a data structure that maps the RIds that belong to that SId into publisher's network locations. All RNs are interconnected in a network known as the rendezvous network.

Figure 2.3. The IBE-PRE scheme of Ateniese and Green

Limitation: -Delay occurs due to two time encryption.

Z. Wang et al[33] proposes scheme in which Attribute Based Encryption (ABE) mechanism is used to create an access policy for the content (AND, OR) operations were used. Here the attribute based scheme is used to hide the access policy of content inside the encryption. It means that only a legitimate user can decrypt the encrypted policy of content. This policy is imposed on the content name rather than the content itself. The concept of trusted third Party 'TTP' was also proposed. The TTP allocate a set of attributes to each network customers according to the customer functional attribute and identity. Before publishing any content by a network entity, the TTP is responsible to allocate global parameter for the information centric network. The network entity can produce attribute which is

 doi:10.20944/preprints202105.0179.v2

then assigned to anyone, interested in this content access. When a content provider wants to transmit the content, it is necessary to accomplish access policy for the content before publishing it. This policy is the arrangement of the related attribute of AND and OR gates. After creating these policies, the content owner generates a random symmetric key which is used to encrypt the publishing content. The content owner also assigns a name to the content. The content real name is digested by using a hash function. The end-user can access the content by their real name through NR (Name based Routing) system. Before using NR, the client uses its attribute to decrypt the real name of content. If these attributes satisfies the hidden policy, it can get the symmetric key that has encrypted the content name. After that, the network name is generated to get the required content through NR system. Limitation:-In this paper the author mentions that they are not focusing on the data integrity of data, without data integrity security is not possible.

K. Xue et al[34] proposed 'SEAF' (Secure Efficient and Accountable Framework) mechanism for ICN. In this scheme the content provider and edge routers perform different tasks; the content provider generates content while the edge router checks the authenticity of end user. The content provider manages users to divide their network user into groups. Different groups have a different access right, i.e. VIP group member can utilize more content then the user of the normal group. The encryption process is performed in two ways i.e. group signature and broadcast encryption. In group signature, the edge router is responsible for the verification/legitimacy of the end user who wants to access any content from the group. Whereas in broadcast encryption, only those users can decrypt the content that has the corresponding access privileges. The SEAF scheme also uses hash chains to convert the expensive signature verification to lightweight hash operation to reduce the computational overhead. The content provider also generates public and private parameter as a group manager. Limitation:-. Delay for the normal user due to grouping .

S. Badsha et al[35] proposes two distinct protocols for the user and content security, CPE2C and PDAC protocol. The protocol Cryptographic Protocol to Exchange the Encrypted Content CPE2C is used to enhance the security of the existing solution and use ABE scheme for content encryption. ABE scheme is used to secure the content from unauthorized user. In the above scheme, the trusted party is used for encryption and decryption. While Privacy-preserving Aggregation over Distributed Content PDAC protocol is used for the aggregation of content using the homomorphic property of public key cryptography. Homomorphic means to apply different mathematical operation like addition, multiplication and subtraction on encrypted data. This protocol also describes how to use smart IOT with CCN architecture. Limitation:-Delay and computational overhead occur due to second times encryption.

C. Bernardini et al[36] proposed security mechanism for both content name and data. Two times encryption and decryption are performed in this scheme. For key generation, the KeyGen is used, which takes the identity of client as input and generate two keys for client i.e. client key (private key) and a proxy key also called (public key) of the client. The client key is securely forwarded to the client to save its private key, which will be used for content decryption. The proxy key is sent to every edge router through which the clients are connected. The proposed scheme immunes both content data and content name from ICN routers to improve the privacy. When a client requests for content, the content provider first generates trapdoor to encrypt the content. The ciphered content is forwarded to the edge router to re-encrypt and store it as shown in figure 4. The edge routers use asymmetric keys for encryption and decryption. The edge router directly connected to end user is responsible for pre-decryption of content and finally, send to the simple cipher content to the requesting client so that it can decrypt the content by its own secret key.

Figure2.4. Content requests and delivery using PrivICN [22].

Limitation:- In this paper author endorse that the proposed mechanism can cause delay and Computational overhead.

Wang et al[37] have designed Session-based Access Control SAC mechanism, in which symmetric key encryption is used by default. The content provider can partly

 doi:10.20944/preprints202105.0179.v2

encrypt the content by encrypting content meta-data (containing details of encryption). For user privacy protection all the sensitive data regarding user privacy is encrypted. This mechanism considered Online Social Network (OSN) as an example for it. A client first registers himself by sharing a symmetric key with OSN service, after the registration process OSN assign a distinctive ID to the client. The user logs-in through this ID to communicate with OSN. A new symmetric key is generated and shared with OSN along with log-in information. Then session ID is assigned to the client by OSN. To upload content, an end user needs to be registered first, and then the client encrypts the content by a previously shared secret symmetric key. After receiving to OSN, the OSN decrypts the object and re-encrypts with a newly generated symmetric key. Other customers request the content using its public name received from OSN. The OSN authorizes the end user and to access to contents and sends back the secure contents, symmetric key decrypts the content. Limitation:-R. Tourani et al [21] have mentioned the limitations due to the two-time encryption performed by edge router delay occur.

R. H. da Silva et al [38] proposed an access control method for ICN in which any client can act as publisher and subscriber of the content thus reduces computational overhead in the applied security keys. Any node which can satisfy an interest will create a group of users and shall act as admin of the group. Any ICN node may join that group through admin. By adding a user to the group, the admin shall ensure assigning a private key to the user. The admin shall securely deliver the private key to the user to use it as the asymmetric encryption key. After becoming a member of the group, each user may securely share content with the fellow members. This method supports fine-grained access control technique for granting and revoking of clients.

Q. Wang et al [39] proposed an access control scheme for ICN by using Shamir Secret share encryption method and proxy Re-encryption techniques. Initially, user gets registration from the Content provider (CP) by sending interest for registration to CP encrypted with the provider public key and user private key. While CP is the data warehouse to fulfil user interest encrypted it by using the Shamir Secret sharing method. This allows users to rebuild the original secret by combining their shares. For this CP generate polynomial and evaluates users and router shares and distribute it with the authorized user as his secret key according to their registration. CP encrypt user to share with user public key and send to a user no intermediate nodes can cache it. The CP then generate enabling block containing an encrypted message and authorized user share by using Shamir Secret polynomial content. The enabling block also signed by CP to guarantee provenance. After this enable block is forwarded to ICN router for caching. The register users can access the enabling block from the router hop containing an encrypted message. Secondly, if subscribed user wants to handover the access content to any near the user. This user re-encrypts the content before sending. The receiver of this content decrypts it with his secret key.

P. He, et al [40] proposed a Lightweight Audit and Secure Access control (LASA) mechanism for ICN. In which content provider divide stored contents into groups, and add GID with each content name according to their security policy. User can also access content other than his group. For user authentication, edge routers are used. Content publisher CP uses broadcast encryption technique for content encryption. CP specifies an access time limit for each client. After publishing content only those user can access the content which has the access privileges for that content, which is specified by CP in form of signature. Due to this signature, the edge router takes decisions whether the client is legitimate or illegitimate for this content. After this audit phase occurs, the ISP responsible by storing signatures to find the client dishonesty regularly. ISP regularly monitor client secret key and inform CP accordingly. CP punishes the dishonest client by reducing access time or prohibits it forever. For all such monitoring, CP offers some extra financial rewards for ISPs. Finally, the client decrypts the content by using GID for right key selection.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2021 doi:10.20944/preprints202105.0179.v2

3. Result and Discussion

3.1. Simulation Tools

A Network Simulator-(NS3) is used for the simulation process of this research work. Inside NS-3 ndn-sim is used, which is designed for implementation of information centric networking.

3.2. Proposed Place of Work and Facilities Available

Department of Computer Science and Bio-Informatics Khushal Khan Khattak University Karak, provide all such sort of nonviolent place and services. Which is obligatory during research work like computer related books, electricity, Internet facility (DSL, Wi-Fi), and also high-quality professional supervision. One individual laboratory (Lab No:03) is specified for research students. Due to these special efforts made by KKKUK for me make this entire research work complete in all admiration within time.

3.3. Plan of Work and Methodology Adopted

Digital Signature for Access Control in information centric network (DSAC-ICN) technique is used for ICN content security. Trusted Third Party (TTP) and Proxy TTP can be used for encryption and key distribution process. The client requests for content by forwarding the request through ICN network to the provider. The provider generates and sends for encryption/ signing to TTP (using digital signature). After encryption, the ciphered content is forwarded to the client through the path on which request have arrived. Network simulator-3is used as simulation tool.

3.4. Research Model

This section contains the proposed research model and technique applied in this framework for security purpose of information centric network. This research model will give an efficient and batter security to content in ICN. This research includes ICN paradigm having ICN routers, an edge router on the client end, Trusted Third Party 'TTP' and proxy 'TTP'. When the client requests for content, the request is forwarded to Content Publisher 'CP' through ICN. Thus content producer generates the content and sends the encrypted content to edage router while the encrypted nonce to the TTP and forwarded the ciphered content to requesting client through ICN as mentioned in detail in chapter 4. TTP send the content name and nonce value 'k' to proxy TTP to satisfy the integrity and confidentiality locally. Another advantage of proxy 'TTP' is to reduce scalability issues.

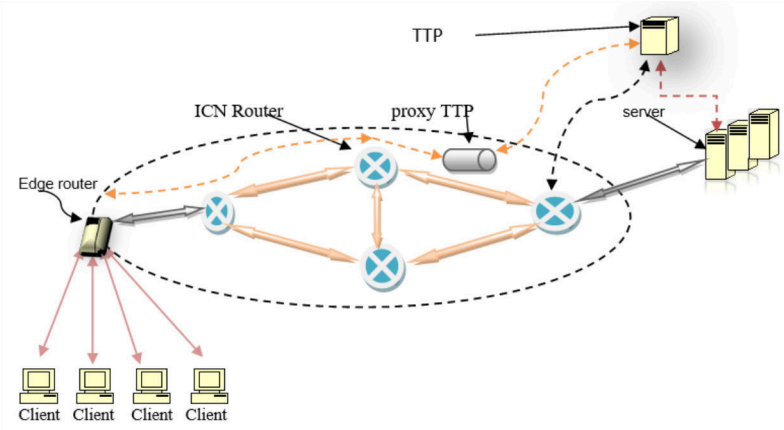

Figure 3. Digital Signature cryptography Based encryption in ICN .

3.5. Simulation Scenarios

In this research study, three simulation scenarios are proposed such as simple scenario, Digital Signature Access Control (DSAC) without TTP and Digital Signature Access Control (DSAC) with TTP. The detail flow diagram for the exchange of content, security keys

 doi:10.20944/preprints202105.0179.v2

and hash number between the consumer and producer through edge routers are briefly explained below.

3.6. Simple Scenario of ICN

As indicated by its name, the simple scenario has client, producer and edge router. The producer generates the content and sends it to the edge router without any kind of encryption. The client put the request for desired the content to the edge router. The edge router provides the content to the client as per request as shown in figure 6.

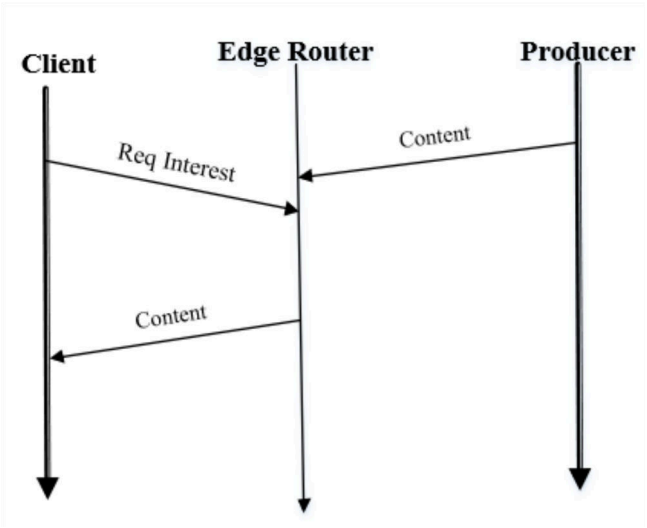

Figure 4. Timeline data flow diagram of ICN in simple scenario .

3.7. Digital Signature Access Control (DSAC) Without TTP

In this scenario, the data exchanged through proper procedure between the producer and client through an edge router in encrypted format as shown in figure 7. All the expected producers and clients will generate the public and private key pairs and will broadcast their private keys. These private keys will be used for calculation of the shared key which will be used for symmetric encryption of data transmitted from producer to the edge router and later on to the client. In the first phase, the Producer will generate the hash value of the content. In the second phase, the content will be encrypted with the shared key. The encrypted data along with hash value is sending to the edge router. The client generates the request for content to the edge router. The edge router sends the encrypted data and its hash value to the client according to the received request for content. The client will first use the hash value to verify the integrity of the received content from the edge router. In case, the integrity test failed to verify the received content, then another request for the same content will be sent to the edge router. On other hand, if the integrity of the received content remainsconstant by verifying through hash value, then the shared key is used to decrypt the received content. This shared key fulfils the authentication and confidentiality requirement of the data exchanged between the producer and client through edge router.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2021 doi:10.20944/preprints202105.0179.v2

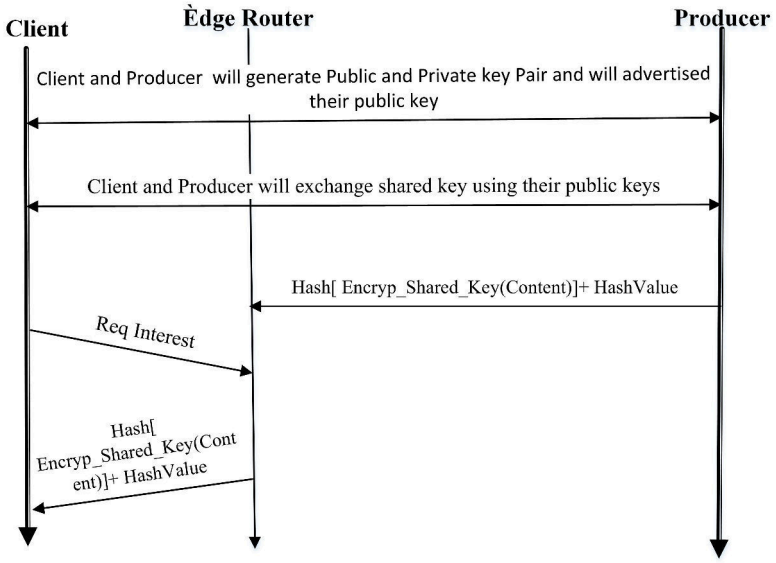

Figure 5. Timeline data flow diagram of ICN using DSAC without TTP .

3.8. Digital Signature Access Control (DSAC) With TTP

In this scenario, the DSAC scheme is used along with Trusted Third Party (TTP) and proxy TTP with the intention to further enhance the security of ICN such as confidentiality, authentication and integrity level as shown in figure 8. TTP and proxy TTP has also improved the scalability of the ICN. The novelty in this scheme is that the producer will generate a random key called nonce and will encrypt the content using the nonce and will generate the hashed value of this encrypted content. The hashed encrypted content and its hash value are transmitted to the edge router. The producer has to encrypt the nonce with a public key of the TTP and Proxy TTP respectively and is sent to the TTP. The TTP will decrypt the encrypted nonce using its private key. At this stage, a nonce is still encrypted with the public key of the proxy TTP. TTP sent this encrypted nonce to the Proxy TTP which will decrypt the nonce with its public key. Now the nonce of the content is available in Proxy TTP. In the next phase, the client has to send the request for content to the edge router. The edge router sent the encrypted content and its hash value to the client. Here, the client will verify the integrity of the received content. The client sends the request nonce to the Proxy TTP. The Proxy TTP will encrypt the Nonce with the public key of the client and will send the encrypted nonce to the client. The client will decrypt the nonce using its private key and will used nonce for decryption of the content.

Here the producer is free from an overload of creating and sharing a shared key with each client. Once the nonce is created and shared with TTP and proxy TTP. Then TTP and proxy TTP is responsible to share the nonce in a secure form with client. This adds an extra level of confidential and authentication level and improves the scalability as compare to the previous scenario.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2021 doi:10.20944/preprints202105.0179.v2

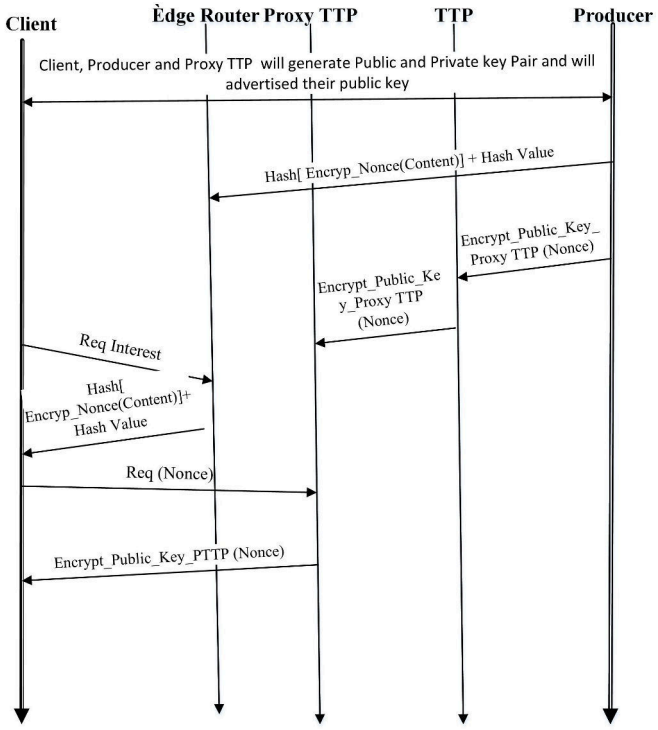

Figure 6. Timeline data flow diagram of ICN using DSAC with TTP .

3.9. Security Analysis

The DSAC with TTP enhances the security of ICN by improving three aspects of security such as authentication, confidentiality and integrity. ICN faces security threats of an attacker that may be producer, client and man-in-middle attacker. These attackers can launch an active attack in the form of impersonation, modification, content/request replay attack or a passive attack such as eavesdropping. Here, the DSAC with TTP is explored concerning following security attacks.

3.10. Man-in-the-middle attacks

The chances of man-in-middle attacks increase if the private key of producer, client, edge router, TTP and proxy TTP get exposed to the attacker. This will help the attacker to decrypt the nonce exchange in encrypted form between the producer and client through TTP, proxy TTP and edge router. It is not possible for an attacker to guess the private keys of the producer, client, edge router, TTP and proxy TTP to find the nonce. In such cases, the attacker tries to send messages for launching a man-in-middle attack are unacceptable and will be detected easily.

3.11. Forward Security

In DSAC, a new random nonce is created for each session. If the attacker gets disclose to nonce accidentally, still he will be not able to decrypt the previous messages or the future messages exchanged between the client and producer. This is not practically feasible to calculate the private keys using the broadcasted public keys in public key cryptography due to usage of large prime integer and modulus function in calculation of private keys.

3.12. Replay Attacks

In attacks, the attacker forwards the sniffed messages of the previous session to the 2nd party for authentication purpose. Such reply attacks will be difficult to launch in DSAC due to the usage of a new nonce number for each session. Replay attacks are most common where the same contents are used repeatedly by the malicious publisher by retransmitting the requests or producer who retransmits the content. On other hand,

 doi:10.20944/preprints202105.0179.v2

both requests and contents are retransmitted by man in the middle attacker. Such types of attacks are prevented by DSAC where the producer and client authenticate each other for each session using the public and private keys and using a new nonce for each session.

3.13. ICN Contents or request modifications

The attacker can launch the integrity attack by changing the requested message of the client or modifying the contents published by the producer. In both cases, the integrity of the generated request or content is verified by the Hash value at the edge router in DSAC. Any kind of tempering in the request or content can easily be detected by the edge router by recalculating the hash value and comparing with received hashed value. In such a case, the client or producer is requested to regenerate content or resend the request.

3.14. Performance Analysis

The performance of DSAC algorithm is evaluated using the parameters such as network overhead, time complexity and space complexity. Each of these performance analysis parameters is briefly discussed below with the intention to find the effect of DSAC on overall ICN architecture.

3.15. Network Overhead

The DSAC make sure the authentication, confidentiality and integrity of the communications between the producer and clients using the four extra messages which is less as compare to other security mechanisms introduced in ICN. Out of these four data securities related messages, only three messages are transmitted between the ICN edge routers and clients which further reduce the network overhead. The security level of DSAC can be increased in future by adding some access control related messages.

3.16. Time Complexity

The message flow chart diagram shows that there is no iteration involved in DSAC. The interaction between the client, producer, edge router, TTP and Proxy TTP follows a simple linear time complexity which is O (1).

3.17. Space Complexity

The DSAC introduced the public, private keys and nonce for enhancing the security for data exchange between the clients and producer. There is a need for little space to store and maintain these keys and shared key (nonce). On other hand, the remarkable increase in the security of the ICN architecture by providing integrity, authentication and confidentiality at cost of light storage overhead is not a big business deal.

3.18. Simulation Environment

Increasing security levels in ICN have directly affected the average access delay. If we add more security level to increase the security of the access control mechanism, the access delay also increases due to processing cost and exchange of extra security related messages. The ICN architecture where each request is honoured with one response also contributes more to the access delay as compare to non-ICN architecture. The security modifications are applied to each request in ICN. DSAC focus on improving the security of ICN at cost of a little bit increase in access delay.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2021 doi:10.20944/preprints202105.0179.v2

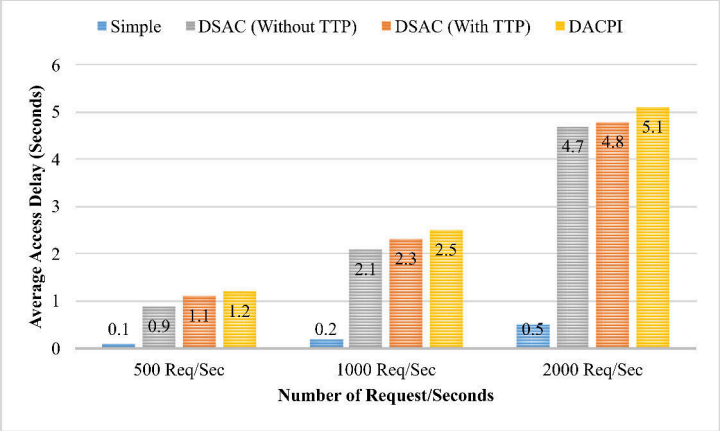

Figure 7. Average Access Delay (Seconds) of Simple, DSAC (Without TTP), DSAC (With TTP) and DACPI.

The simulation was conducted using the ndn-SIM which provides ICN within the NS3. The experimental ICN consist of 5 clients, 1 Producer/publishers, and 6 routers as shown in Figure 4.4. Three simulation scenarios were designed with respect to an increasing number of requests per seconds that is 500 request/seconds, 1000 requests/ seconds and 2000 requests/seconds. In each sub scenario, the three security protocols were simulated such as Decentralized Access Control Protocol for ICN architectures (DACPI) protocol [26], DSAC without TTP and DSAC with TTP along with the simple scenario. The simple scenario is the by default one that has no access control mechanism. The simulation results show that DSAC has less average access delay as compare to the DACPI in all the three scenarios such as 500 request/seconds, 1000 requests/seconds and 2000 requests/seconds. DSAC without TTP has outperformed the DSAC with TTP by having less average access delay. The three access control mechanism (DACPI, DSAC without TTP and DSAC with TTP) have observed increased in the average access delay due to exchange of extra messages and processing delay of cryptographic schemes for enhancing the access security. This average access delay also increases with an increase in the number of requests per seconds.

3.18.1. Authentication

The authentication process can be divided into two different phases "Identification" and "Actual Authentication". In the identification phase, user identity is offered in the form of a user ID. Then the security system will then ensure all the figurative objects that it knows and can find the truthful one of which the genuine user is at present applying. Once this is done the user has been identified. Authentication means to recognize or determine someone or something in real, who declare itself be legitimate. It is the procedure/technology to grant access control for information/data by configuring it to see where the user's tribute matches the credential in a database of authoritative users or a data authentication server. Authentication always checked at the start of the application, before the permission and throttling checks occur, and before any other code is allowed to process.

3.18.2. Confidentiality

Confidentiality means something in full confidence or in secret or the state of knowledge being held in confidence. Confidentiality also refers to the people who are authorized to do so can gain access to sensitive data. Confidentiality failure means to preserve the confidentiality of someone who should not have the access privileges to get it through intentional behavior or by an accidentally called breach. In the context of computer networking confidentiality allows only legitimate users to access sensitive and ciphered content/data. Some special mechanisms are used for ensuring confidentiality and safeguard of data/content from harmful intruders.

 doi:10.20944/preprints202105.0179.v2

3.18.3. Integrity

Integrity in the context of computer network means the overall completeness of accuracy and consistency of data. It is a must before sending data through the network to impose integrity necessarily, and it is possible by applying error checking and correction n protocol. Simply when the receiving data is not similar as the data sent, it means there is some problem occurs. Most of the researchers work on to improve the integrity of data, which is roughly important for both producer and client.

3.19. Summary

This portion is taken as a whole and comprehensive approach, which can define the complete procedure of this research work in summarized form. This research scheme performs security enhancement in ICN content by using RSA and Hash function. Trusted third party TTP and proxy TTP also used for storing the decryption key as well as for consumer authentication. This scheme mainly focuses on the authentication, confidentiality and integrity of data and consumer authentication. As from the result, it is clear that the result is excellent as compare to the previous work. NS-3 simulator is used to simulate the complete interest in sending, receiving, encryption authentication of consumers.

3.20. Discussion

The discussion intends to understand and explain the importance of this research in light of what was known to the researcher before this research problem being investigated and want to find more batter result in this field. So it is clear from the past research paper that each and everyone had sent the decryption key on the same route on which the content is to be sent, which may possibly be a case to find the decryption key by some malicious node easily. In ECAC and DACPI, Public key cryptgraphy and random generated number was used, but they endorse that due to this technique some delay and extra storage on both producer and receiver side are necessary for storing nonce values [26]. Some of the above papers uses attribute base encryption technique, but still information Centric Networking architecture wants some batter security plan and model because of their high bandwidth.

In light of the above-mentioned problems, this research uses a good research scheme for ICN content security by using Digital Signature and Hash function for encryption and decryption. The producer generate content, encrypt it by using digital signature and hash value and then send the hash value to the trusted third party and proxy TTP. On the request of client, the encrypted ciphered content is forwarded to client through ICN and edge router. While the content name along with ciphered nonce hash value is forwarded to proxy TTP. When the edge router receives cipher content it requests for decryption hash value for the same content from proxy TTP and will be provided to edge router for further processing. Finally, the clients receive the content and decrypt it to access.

In this entire scheme after encryption, the content is forwarded through ICN architecture, each and every route capture single copy of the forwarded content and sends the content back on the path from where it receives the request for the same content. The router stores the path from which it accepts the request. Therefore, every router has the ability to store the content for a limited time to fulfil the future request for the same content local, which is the only and novel aspect of information centric networking not used before any networking architecture.

This research scheme consists of RSA (Rivest Shamir Adleman) and Hash function based encryption/decryption techniques. RSA provides batter security for ICN content by using 1024 bits key size, which is quite difficult from someone to hack or theft the same decryption key easily. RSA is the name used for the best security mechanism. While the hash function is used for security as well as confidentiality and integrity of the content, which is very necessary for the client before accepting any ciphered content. This is why

 doi:10.20944/preprints202105.0179.v2

this research work claims that this scheme is secure as compared to previous work already done in this field. This research focusing on the main issues occur/related to ICN content due to the past work like scalability, sending of the decryption key in a separate channel, confidentiality and integrity.

Network Simulator-3 (ndn-Sim) is used to simulate for implementation of the proposed access control security mechanism. NS-3 is one of the latest and quite suitable for the ICN architecture because most of the issues which are not possible in any other network simulator to be performed successfully according to the required solution. Inside NS-3 a name data network simulation (ndn-Sim), this was specially designed for Information Centric Networking architecture like Producer and Subscriber. This work first checks on NS-2 simulator but there is a lot of problems and possibly not able to solve the complete simulation of this research.

4. Conclusion and Recommendations

4.1. Conclusion

Digital Signature for Access Control in information centric network (DSAC) technique is proposed to provide batter access control solution for information centric network. The proposed solution based on Trusted Third Party (TTP) and proxy TTP node. The motivation behind proxy TTP node is to perform authentication, confidentiality and integrity of data and consumer authentication issues for a client locally. The client request for content through the edge router, the request sent to the content producer through ICN. The content producer generates the content and encrypts it using Digital Signature and hash function value 'k' to prevent the content from unauthorized user access and forward the encrypted content to end user through ICN. The content name and hash value of 'k' are forward to TTP and proxy TTP to satisfy the consumer authentication issues locally.

4.2. Recommendations

Information centric network supports high data-rate and needs high security as compared to the existing conventional system. For the same scheme use of Elliptic curve encryption is much better, because of shorter key size and higher security level. The decryption key for cached content may be separately sent to every content consumer, such that ciphered content and decryption key are not cached at the same place (means through separate medium). By using Elliptic curve it is easy to secure the IOT devices data, because of low computational complexity [**?**].

1. Bosunia, M.R.; Hasan, K.; Nasir, N.A.; Kwon, S.; Jeong, S.H. Efficient data delivery based on content-centric networking for Internet of Things applications. *International Journal of Distributed Sensor Networks* **2016**, *12*, 1550147716665518.
2. Wang, Y.; Xu, M.; Feng, Z.; Li, Q.; Li, Q. Session-based access control in information-centric networks: Design and analyses. 2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC). IEEE, 2014, pp. 1–8.
3. Ghali, C.; Tsudik, G.; Wood, C.A. When encryption is not enough: privacy attacks in content-centric networking. Proceedings of the 4th ACM Conference on Information-Centric Networking, 2017, pp. 1–10.
4. Renault, É.; Ahmad, A.; Abid, M. Access control to objects and their description in the future network of information. *Journal of information processing systems* **2010**, *6*, 359–374.
5. Li, B.; Huang, D.; Wang, Z.; Zhu, Y. Attribute-based access control for ICN naming scheme. *IEEE Transactions on Dependable and Secure Computing* **2016**, *15*, 194–206.
6. Zhang, Q.Y.; Wang, X.W.; Huang, M.; Li, K.Q.; Das, S.K. Software defined networking meets information centric networking: A survey. *IEEE Access* **2018**, *6*, 39547–39563.
7. AbdAllah, E.G.; Hassanein, H.S.; Zulkernine, M. A survey of security attacks in information-centric networking. *IEEE Communications Surveys & Tutorials* **2015**, *17*, 1441–1454.

8. AbdAllah, E.G.; Zulkernine, M.; Hassanein, H.S. DACPI: A decentralized access control protocol for information centric networking. 2016 IEEE International Conference on Communications (ICC). IEEE, 2016, pp. 1–6.
9. Tan, X.; Huang, C.; Ji, L. Access control scheme based on combination of blockchain and XOR-coding for ICN. 2018 5th IEEE international conference on cyber security and cloud computing (CSCloud)/2018 4th IEEE international conference on edge computing and scalable cloud (EdgeCom). IEEE, 2018, pp. 160–165.
10. Chu, W.B.; Wang, L.F.; Jiang, Z.J.; Chang, A.C.C. Protecting user privacy in a multi-path information-centric network using multiple random-caches. *Journal of Computer Science and Technology* **2017**, *32*, 585–598.
11. Li, J.; Liu, B.; Wu, H. Energy-efficient in-network caching for content-centric networking. *IEEE Communications Letters* **2013**, *17*, 797–800.
12. Kuriharay, J.; Uzun, E.; Wood, C.A. An encryption-based access control framework for content-centric networking. 2015 IFIP networking conference (IFIP networking). IEEE, 2015, pp. 1–9.
13. Chu, W.B.; Wang, L.F.; Jiang, Z.J.; Chang, A.C.C. Protecting user privacy in a multi-path information-centric network using multiple random-caches. *Journal of Computer Science and Technology* **2017**, *32*, 585–598.
14. Zheng, Q.; Wang, G.; Ravindran, R.; Azgin, A. Achieving secure and scalable data access control in information-centric networking. 2015 IEEE International Conference on Communications (ICC). IEEE, 2015, pp. 5367–5373.
15. Kuriharay, J.; Uzun, E.; Wood, C.A. An encryption-based access control framework for content-centric networking. 2015 IFIP networking conference (IFIP networking). IEEE, 2015, pp. 1–9.
16. Li, J.; Liu, B.; Wu, H. Energy-efficient in-network caching for content-centric networking. *IEEE Communications Letters* **2013**, *17*, 797–800.
17. Nunes, I.O.; Tsudik, G. KRB-CCN: lightweight authentication and access control for private content-centric networks. International Conference on Applied Cryptography and Network Security. Springer, 2018, pp. 598–615.
18. Vural, S.; Wang, N.; Navaratnam, P.; Tafazolli, R. Caching transient data in internet content routers. *IEEE/ACM Transactions on Networking* **2016**, *25*, 1048–1061.
19. Quevedo, J.; Corujo, D.; Aguiar, R. Consumer driven information freshness approach for content centric networking. 2014 IEEE conference on computer communications workshops (INFOCOM WKSHPS). IEEE, 2014, pp. 482–487.
20. Meddeb, M.; Dhraief, A.; Belghith, A.; Monteil, T.; Drira, K.; AlAhmadi, S. Cache freshness in named data networking for the internet of things. *The Computer Journal* **2018**, *61*, 1496–1511.
21. Tourani, R.; Misra, S.; Mick, T.; Panwar, G. Security, privacy, and access control in information-centric networking: A survey. *IEEE communications surveys & tutorials* **2017**, *20*, 566–600.
22. Buchmann, J. *Introduction to cryptography*; Springer Science & Business Media, 2013.
23. Aufa, F.J.; Affandi, A.; others. Security system analysis in combination method: RSA encryption and digital signature algorithm. 2018 4th International Conference on Science and Technology (ICST). IEEE, 2018, pp. 1–5.
24. Hwang, T.; Luo, Y.P.; Gope, P.; Liu, Z.R. Forward/backward unforgeable digital signature scheme using symmetric-key crypto-system. 2016 International Computer Symposium (ICS). IEEE, 2016, pp. 244–247.
25. Ullah, R.; Umar, A.I.; ul Amin, N.; others. Blind signcryption scheme based on elliptic curves. 2014 Conference on Information Assurance and Cyber Security (CIACS). IEEE, 2014, pp. 51–54.
26. AbdAllah, E.G.; Zulkernine, M.; Hassanein, H.S. Preventing unauthorized access in information centric networking. *Security and Privacy* **2018**, *1*, e33.
27. Li, Q.; Sandhu, R.; Zhang, X.; Xu, M. Mandatory content access control for privacy protection in information centric networks. *IEEE Transactions on Dependable and Secure Computing* **2015**, *14*, 494–506.
28. Zheng, Q.; Wang, G.; Ravindran, R.; Azgin, A. Achieving secure and scalable data access control in information-centric networking. 2015 IEEE International Conference on Communications (ICC). IEEE, 2015, pp. 5367–5373.
29. Fotiou, N.; Polyzos, G.C. Securing content sharing over ICN. Proceedings of the 3rd ACM Conference on Information-Centric Networking, 2016, pp. 176–185.

30. Misra, S.; Tourani, R.; Natividad, F.; Mick, T.; Majd, N.E.; Huang, H. AccConF: An access control framework for leveraging in-network cached data in the ICN-enabled wireless edge. *IEEE transactions on dependable and secure computing* **2017**, *16*, 5–17.
31. Misra, S.; Tourani, R.; Majd, N.E. Secure content delivery in information-centric networks: Design, implementation, and analyses. Proceedings of the 3rd ACM SIGCOMM workshop on Information-centric networking, 2013, pp. 73–78.
32. Fotiou, N.; Alzahrani, B.A. Rendezvous-based access control for information-centric architectures. *International Journal of Network Management* **2018**, *28*, e2007.
33. Li, B.; Wang, Z.; Huang, D.; Zhu, Y. Toward privacy-preserving content access control for information centric networking. Technical report, ARIZONA STATE UNIV TEMPE OFFICE OF RESEARCH AND SPONSORED PROJECT ADMINISTRATION, 2014.
34. Xue, K.; Zhang, X.; Xia, Q.; Wei, D.S.; Yue, H.; Wu, F. SEAF: A secure, efficient and accountable access control framework for information centric networking. IEEE INFOCOM 2018-IEEE Conference on Computer Communications. IEEE, 2018, pp. 2213–2221.
35. Badsha, S.; Khalil, I.; Yi, X.; Atiquzzaman, M. Designing privacy-preserving protocols for content sharing and aggregation in content centric networking. *IEEE Access* **2018**, *6*, 42119–42130.
36. Bernardini, C.; Marchal, S.; Asghar, M.R.; Crispo, B. PrivICN: Privacy-preserving content retrieval in information-centric networking. *Computer Networks* **2019**, *149*, 13–28.
37. Wang, Y.; Xu, M.; Feng, Z.; Li, Q.; Li, Q. Session-based access control in information-centric networks: Design and analyses. 2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC). IEEE, 2014, pp. 1–8.
38. da Silva, R.H.; Da Costa Cordeiro, W.L.; Gaspary, L.P. A scalable approach for managing access control in Information Centric Networks. 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2017, pp. 89–97. doi:10.23919/INM.2017.7987268.
39. Wang, Q.; Li, W.; Qin, Z. Proxy Re-Encryption in Access Control Framework of Information-Centric Networks. *IEEE Access* **2019**, *7*, 48417–48429. doi:10.1109/ACCESS.2019.2908009.
40. He, P.; Wan, Y.; Xia, Q.; Li, S.; Hong, J.; Xue, K. LASA: Lightweight, Auditable and Secure Access Control in ICN with Limitation of Access Times. 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1–6. doi:10.1109/ICC.2018.8422829.

==========