A NOVEL ACCESS CONTROL SCHEME FOR INFORMATION CENTRIC NETWORK

[1]M.NAGAJYOTHI [2]DR. RISHI SAYAL
[1,2]Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad
[1]Assistant Professor, [2]Professor

ABSTRACT

In the basic networking schemes, a network entity can access some information content which may lead to unauthorized access of the data. It is done by locating server and connecting it to provide a service which follows any network routing protocol, which results to tightly associated information with the server location. To make the connection condition as a major factor to the network, we have to modify the entire network centered on the connections between content consumers with their content providers, in this paper we are proposing ICN architecture by analyzing the fact that the network traffic is utilized more in the case of file sharing especially video sharing. In this ICN architecture, the main focus is to be transferring from consumer-server connections to consumer-content connections. Hence, the network changes to identify authentic content copies instead of identifying the content owner's address. In this regard, the consumers do not need to know where the content locates, i.e. the IP address of the content owner. The content name is enough to direct the consumer to the content copy. When content owners publish their content, it can be copied and stored in the network using network caches. This design enables content being efficiently delivered to the consumers.

Keywords: Information Centric Network, naming, files, access, and control.

1. INTRODUCTION

ICN architectures focus on contents or information objects and their properties in the network. ICN is also concerned about receiver interests. In order to achieve these goals, ICN relies on location independent naming, in network caching and name-based routing. In ICN, senders do not send content directly to receivers. A sender publishes advertisement messages to tell the network that it has some content to share, without necessarily knowing who may be interested in it. On the other side, a receiver declares its interest for some content, not necessarily knowing the senders who have published this content. The ICN network makes a delivery path from the sender to the receiver when there is a match between sender's publication and receiver's subscription. Finally, the content is transferred to the receiver.

2. SCOPE OF THE WORK

In this work, the Survey of attacks is analyzed and identified to a few existing ICN architectures. There are some specific attacks that have an impact on ICN which may be considered as generic attacks on networks. It also provides taxonomy of these generic attacks in ICN architecture and shows the relation between ICN attacks and unique ICN attributes. We provide achievability schemes and outer bounds for the secure network coding setting, where the edges are subjected to packet erasures. It also provides facility for public feedback of the channel state is to be available for both Eves and also to the legitimate network nodes.

2.1. Related Work

The paper [2] proposed a routing scheme for content based networking. Content-based network is a communication network that features a new advanced communication model where messages are not given explicit destination addresses, and where the destinations of a message are determined by matching the content of the message against selection predicates declared by nodes.. The routing scheme we propose uses a combination of a traditional broadcast protocol and content based routing protocol. We then detail the content-based routing protocol, highlighting a set of optimization heuristics. We also present the results of our evaluation, showing that this routing scheme is effective and scalable.

The paper [3] has proposed that the internet has evolved greatly from its original incarnation. For instance, the vast majority of current Internet usage is data retrieval and service access, whereas the architecture was designed around host-to-host applications such as telnet and FTP. Moreover, the original Internet was a purely transparent carrier of packets, but now the various network stakeholders use middle boxes to improve security and accelerate applications. To adapt to these changes, we propose the Data-Oriented Network Architecture (DONA), which involves a clean-slate redesign of Internet naming and name resolution.

The paper [4] proposed several projects propose an information-centric approach to the network of the future. Such an approach makes efficient content distribution possible by making information retrieval host-independent and integrating into the network storage for caching information. Requests for particular content can, thus, be satisfied by any host or server holding a copy. The current security model based on host authentication is not applicable in this context. Basic security functionality must instead be attached directly to the data and its naming scheme. A naming scheme to name content and other objects that enables verification of data integrity as well as owner authentication and identification is here presented. The naming scheme is designed for flexibility and extensibility, e.g., to integrate other security properties like access control. The requirements for the naming

scheme and an analysis showing how the proposed scheme fulfills them are presented. Experience with prototyping the naming scheme is also discussed. The naming scheme builds the foundation for a secure information-centric network infrastructure that can also solve some of the main security problems of today's Internet.

The paper [6] proposed that Network use has evolved to be dominated by content distribution and retrieval, while networking technology still speaks only of connections between hosts. Accessing content and services requires mapping from the what that users care about to the network's where. We present Content-Centric Networking (CCN) which treats content as a primitive – decoupling location from identity, security and access, and retrieving content by name. Using new approaches to routing named content, derived heavily from IP, we can simultaneously achieve scalability, security and performance. We implemented our architecture's basic features and demonstrate resilience and performance with secure file downloads and VoIP calls.

The paper proposed [7] In-network caching necessitates the transformation of centralized operations of traditional, overlay caching techniques to a decentralized and uncoordinated environment. Given that caching capacity in routers is relatively small in comparison to the amount of forwarded content, a key aspect is the distribution of content among the available caches. In this paper, we are concerned with decentralized, real-time distribution of content in router caches. to: i) leave caching space for other flows sharing (part of) the same path, and ii) fairly multiplex contents of different flows in caches along a shared path. We compare our algorithm against universal caching and against schemes proposed in the past for Web-Caching architectures, such as Leave Copy down (LCD). Our results show reduction of up to 20% in server hits, and up to 10% in the number of hops required to hit cached contents, but, most importantly, reduction of cache-evictions by an order of magnitude in comparison to universal caching.

The paper proposed[8] that Information is the building block of Information Centric Networks (ICNs). Access control policies limit information dissemination to authorized entities only. Defining access control policies in an ICN is a non-trivial task as an information item may exist in multiple copies dispersed in various network locations, including caches and content replication servers. In this paper we propose an access control enforcement delegation scheme which enables the purveyor of an information item to evaluate a request against an access control policy, without having access neither to the requestor credentials nor to the actual definition of the policy. Such an approach has multiple merits: it enables the interoperability of various stakeholders, it protects user identity and it can set the basis for a privacy preserving mechanism. An implementation of our scheme supports its feasibility.

Bharat k *at el.* proposed that Mobile peer-to-peer networks of aerial vehicles (AVs) have become significant in collaborative tasks including military missions and search and rescue operations. However, the nature of the communication between the nodes in these networks makes the disseminated data prone to interception by malicious parties, which could cause serious harm for the designated mission of the network. In this paper, we propose an approach for secure data dissemination in a mobile peer-to-peer network, where the data disclosed to a particular node in the network depends on the trustworthiness of that node as well as the matching of policies of the data source and destination. We also discuss filtering techniques for dissemination of sensitive data in such networks.

The paper 10] proposed that In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Cipher text-Policy Attribute-Based Encryption. while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

Bengt Algren Christian Dannewitz Claudio Imbrenda proposed that The development of the Information-Centric Networking (ICN) concept is one of the signi_cant results of different international Future Internet research activities. In this concept, the principal paradigm is not end-to-end communication between hosts as in the current Internet architecture Corresponding network architectures can leverage in-network storage, multiparty communication through replication and interaction models such as publish-subscribe to provide general platforms for communication services that are today only available in dedicated systems such as peer-to-peer overlays and proprietary content-distribution networks.

The paper [11] proposed in many applications, it is desired to dynamically establish temporary multicast groups for secure message delivery. It is also often the case that the group membership information itself is sensitive and needs to be well protected. However, existing solutions either fail to address the issue of membership anonymity or do not scale well for dynamically established groups. In this paper, we propose a highly scalable solution for dynamical multicast group setup with group membership anonymity. In our design, multicast groups are specified through group member attributes. As these attributes are potentially able to be shared by unlimited number of group members, our proposed scheme scales well. Also, high level of membership anonymity is guaranteed such that every group member knows nothing but his own group membership only. The complexity of our proposed scheme in terms of computational overhead and cipher text size is O(n), where n is the number of attributes and independent to the group size.

3. MODULES

This work comprises the following six modules:

1. User interface design.
2. Data upload
3. Key generate
4. Attackers

5. Encryption and packets making
6. Key access to receiver

3.1. User Interface Design

This is the first module of our project. The important role for the cloud user is to move from login window to cloud user window. This module is created for security purpose. In login page we have to enter user id and password. It will check whether the username and password are valid or not. If we enter any invalid username or password we can't move to user window it will shows an error message. So we are preventing an unauthorized user to enter the user window. It will provide a good security for our project. In our project we are using JSP for creating design. Here we validate the login user and server authentication.

3.2. Data Upload

This is the module for uploading consumer's files or documents into the virtual machines. They serve a dual purpose as they can introduce high-level policies and assist in administration tasks. Reduce Dist. enforces the high-level policy of clustering VMs of the same user on hosts that may not be far apart in terms of network hops. The user send the message to destination security send the Data so upload the file or Data. Given that we rely on network services for our most security-critical data. A source will send a message to number of receivers securely over a network in the presence of a passive eavesdropper with unit-capacity edges.

3.3. Key Generate:

This module is for creating the Key Generate Data or documents into the virtual machines. They serve a dual purpose as they can introduce high-level policies and assist in administration tasks. Secure message transfer over error-free networks, as well as single point-to-point network with state feedback. It inserts into network linear combinations of the message and the random packets. We design likelihood schemes that can offer high secure message sending rate when compared to the alternative of channel coding then followed by secure network coding for an error-free network.

3.4. Attackers

In this module the user itself act as attackers with the list of available attacks they can produce. If they want data to retrieve in normal mode they can retrieve it if User want any attacks to happen to that file they can choose which attack has to happen. Network Attacks namely Naming, Routing, Cache, Other Miscellaneous Attacks may cause harm to your Files. Naming Attack i.e., the Attacker may delete the request that the user send to server. Routing Attack i.e., the Attacker may change the path of the receiver. Cache Attacks i.e., the Attacker make a unwanted updates so that it causes to workload. Finally Miscellaneous Attacks ie., the Attacks happens during downloading time user may not able to download the file he/she wants.

3.5. Encryption and Packet Making:

This module is to Secure the Data that comes from the source to Destination. If unauthorized receiver gets the Data so the data Encryption method introduced in this session. This is main use on Data split. It sends the receiver and avoids the missing data or Field in the system. The main use is to send secure data from user to receiver. It inserts network linear combinations of the message and the random packets.

3.6. Key Access to Receiver:

We have to consider secure network coding in a framework where only security against computationally bounded adversaries or statistical security required. Data will be highly securable. Packets sent in parallel on different edges are always independent. Secure message transfers over error-free networks, and single point-to-point network with state feedback. Source will send a message to number of receivers securely over a network in the presence of a passive eavesdropper with unit-capacity edges.

4. TECHNIQUE USED OR ALGORITHM USED

To evaluate the data reliability, we have to focus on some problems, which are done by proposing a model by means of evidence theory. To model uncertainty and richness to be achieved for the full capacity, operators need to be combined in the model.

4.1. Multiple Keywords Searchable Encryption

We have been proposed two MRSE schemes based on the similarity measure of "coordinate matching" while meeting different privacy requirements in two different threat models .We investigate some further enhancements of our ranked search mechanism to support more search semantics and dynamic data operations. Deep analysis of the proposed scheme ensures that the algorithm introduced a low overhead for communication

5. FUTURE ENHANCEMENT

In future, the internet comes with high necessities of information dissemination, which motivate the research community to find alternative solutions. ICN, as one of these solutions focuses on contents to provide a scalable and efficient content delivery.

6. APPLICATION

LDO is the keystone of The Semantic Web, yet there still very few commercial LDO apps. In the latest issue of No dualities, a magazine about the Semantic Web by UK Company Tails, there is an article by Tails CTO Ian Davis about the state of Semantic Web applications.

CONCLUSION

We proposed a novel access control approach for ICN naming scheme. This scheme is based on a new design of ABE-based algorithm and the content names are protected based on attributes. Our work also proposes a new ontology-based scheme to implement a better functionality for flexible attribute management with significant performance gains to maintain efficient storage costs and less consumption of time. High level Security is achieved with this scheme by the help of CP-ABE, but with attribute anonymity privacy might not be guaranteed with the policy. Experiments and analysis confirm the effectiveness and efficiency of our scheme and design.

REFERENCES:

[1] Cisco, "Cisco visual networking index: forecast and methodology, 2012-2017," 2013.
[2] A. Carzaniga, M. Rutherford, and A. Wolf, "A routing scheme for content-based networking," in INFOCOM 2004.
[3] T. e. Koponen, "A data-oriented (and beyond) network architecture," in Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communications, 2007.
[4] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, "Secure naming for a network of information," in INFOCOM 2010.
[5] N. Fotiou, P. Nikander, D. Trossen, and G. Polyzos, "Developing information networking further: From psirp to pursuit," ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2012.
[6] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in Proceedings of the 5th international conference on Emerging networking experiments and technologies, 2009.
[7] I. Psaras, W. K. Chai, and G. Pavlou, "Probabilistic in network caching for information-centric networks," in Proceedings of the second edition of the ICN workshop on Information-centric networking, 2012.
[8] N. Fotiou, G. F. Marias, and G. C. Polyzos, "Access control enforcement delegation for information-centric networking architectures," in Proceedings of the second edition of the ICN workshop on Information-centric networking, 2012.
[9] S. Singh, "A trust based approach for secure access control in information centric network," International Journal of Information and Network Security (IJINS), 2012.
[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertextpolicy attribute-based encryption," in Proceedings of the IEEE Symposium on Security and Privacy, 2007.
[11] S. Yu, K. Ren, and W. Lou, "Attribute-based on-demand multicast group setup with membership anonymity," in Proceedings of the 4th international conference on Security and privacy in communication netowrks, 2008.
[12] A. Lewko and B. Waters, "Decentralizing attribute based encryption," in Proceedings of the 30th Annual international conference on Theory and applications of cryptographic techniques: advances in cryptology, 2011.
[13] S. Arianfar, T. Koponen, B. Raghavan, and S. Shenker, "On preserving privacy in content-oriented networks," in Proceedings of the ACM SIGCOMM workshop on Information-centric networking, 2011.
[14] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor specified access structures," in Proceedings of the 6th international conference on Applied cryptography and network security, 2008.
[15] D. Huang, Z. Zhou, and Z. Yan, "Gradual identity exposure using attribute-based encryption," in Social Computing (SocialCom), IEEE Second International Conference on, 2010.
[16] S. Bechhofer, F. v. Harmelen, J. Hendler, I. Horrocks, D. L. McGuinness, P. F. Patel-Schneider, and L. A. Stein. (2004) Owl web ontology language reference.
[17] (2008) Sparql query language for rdf. [Online]. Available: http://www.w3.org/TR/rdf-sparql-query/
[18] B. Li, Z. Wang, and D. Huang, "An efficient and anonymous attribute-based group setup scheme," in Proceedings of GLOBECOM, 2013.
[19] P. Ashwin. (2014) Ontology based attribute management for abac. [Online]. Available: http://ontology-ABAC. mobicloud.asu.edu
[20] L. Cheung and C. Newport, "Provably secure ciphertext 2014 IEEE Conference on Communications and Network Security 398 2016 policy abe," in Proceedings of the 14th ACM conference on Computer and communications security, 2007.