e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 12, December 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712035

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

User Data Centric Authentication for Network Data Retrieval

D. Srinivas[1], E. Poojitha[2], A Shashi Kumar[3], A Sriharsha Reddy[4]

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India[1]

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India[2,3,4]

ABSTRACT: Big data raises a strong demand on a network infrastructure to support the secure and efficient data retrieval with in-network caching. Information-Centric Networking (ICN) is an emerging approach to satisfy this demand, where big data are ubiquitously cached at the intermediate physical entities (IPEs) in the network and users retrieve the published data from the close copy holders. For the ICN, the unpredictability of users, IPEs, copy holders, and publishers during in-network big data retrievals poses a challenge to design a data-centric authentication mechanism to inhibit the malicious users to flood data requests and prevent the fake data from being cached and provided. However, the existing work only provides the authentications between users and publishers and suffers from the delay enlargement problem. To solve these problems, we design a trust model, namely a suspension-chain model (SCM), which is a trust chain that seamlessly merges certificate authority (CA)-based trust and neighbour-based trust. Based on SCM, we propose the DC AUTH integrating certificate collection and packet forwarding, where the suspension certificate chain can be constructed for realizing any authentication to the unpredictable users/IPEs/publishers without accessing servers. Extensive simulations have been conducted to compare DC AUTH with the existing work, which shows that delay can be greatly reduced and attacks can be efficiently prevented by DC AUTH.

I. INTRODUCTION

Billions of people with mobile devices and small things, such as sensors, actuators, and robots, are generating tremendous amounts of data. This is known as big data, and is characterized by five aspects: volume, variety, velocity, value, and complexity. Big data have attracted wide attention to develop business applications, such as the Internet of Things (IoT). One of the foundations for these services is to efficiently retrieve these big data which is currently designed based on end-to end communications within the Internet. That is, most services are implemented based on centralized servers/clouds, and big data need to be distributed from the distant server/cloud to users, possibly through similar paths. Because of this, the current big-data retrievals effect large redundant and duplicate traffic, as well as large latency. To cope with the retrieval of a huge amount of data, the network designs for big data are indispensable, and the architectures supporting in-network big-data retrieval, such as Information Centric Network (ICN) and Named-Data Network (NDN), have been proposed for content-centric applications. In these networks, big data are cached at the Intermediate Physical Entities (IPEs), such as routers, close to users for reducing delay and redundant bandwidth consumption. However, in-network big-data retrieval leads the network to be seriously vulnerable to a variety of attacks, such as malicious-request attacks, and data-poisoning attacks. In a malicious-request attack, adversaries impersonate users to flood data requests (or Interests), thereby causing the network to malfunction. In a data-poisoning attack, adversaries impersonate copy holders or publishers to provide fake data. This form of attack can quickly pollute the IPE caches as the virus spreads, because IPEs cache the fake data, redistribute them, and other intermediate IPEs re-cache them. It finally consumes much in-network caching storage and prevents users from retrieve the correct big data. Combatting these attacks is much more difficult for in-network big-data retrieval than it is on the Internet, where the users and server(s) providing the data are pre-determined and end-to-end trust 1 is easily established. Unlike on the Internet, the unpredictability with which copy holders provide big data, IPEs cache big data, and users request big data leads to great difficulty in inhibiting malicious-request attacks and data-poisoning attacks. To prevent cache poisoning, users and IPEs need to verify data before storing or caching them. If the data are found to be fake, the copy holder providing the data and the path to retrieve the data should also be discovered in order to disable the further spread of that fake data. To prevent malicious-request attacks, copy holders should verify the identities of the users. That is, the

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

authentication from any user/IPE to the copy holders/publishers or from any IPE to users is required to be provided during the in-network big data retrieval, which is simply called data-centric authentication in this paper. The related work on secure in-network big-data retrieval can be classified as Internet Protocol (IP) based solutions and ICN-based solutions. However, both approaches only provide the authentications between the users and publishers without considering data-centric authentication, and are unable to prevent the malicious-request and data-poisoning attacks. Furthermore, they rely on centralized servers to acquire certificates, thereby increasing authentication delays, which we refer to herein as the delay-enlargement problem. To solve these problems, we propose a model of data-centric authentication with suspension chain (DC AUTH) for secure in network big-data retrieval. In DC AUTH, packet forwarding and suspension certificate chain construction are seamlessly integrated to efficiently realize data centric authentication. To the best of our knowledge, this is the first study to address the issue of trust establishment among unpredictable entities during data acquisition. It can also be widely applicable for secure routing and secure transport during in-network big-data retrieval. The following new properties distinguish the present study from existing works.

- 1 A suspension-chain model (SCM) is proposed as the trust model, where the neighbour trust-based certificate chain is suspended by certificate authority (CA)-based trust. It fundamentally enables the realization of data-centric authentication.

- Forwarding-integrated hop-by-hop certificate collection together with the adaptive replacement for parts of chain with highly trustworthy certificates is proposed to construct the trustworthy suspension certificate chain based on SCM. It avoids reliance on centralized server(s) for chain construction and solves the delay-enlargement problem.

- DC AUTH smoothly extends the authentication from the physical entities to the logic entities. It breaks the barrier between networking and big-data applications, which follows the data-centric approach. Security analysis shows that DC AUTH can satisfy the security design requirements. Extensive simulations show that DC AUTH greatly reduces delays compared to the existing PKI-NDN scheme, and it can also efficiently prevent the malicious-request and data poisoning attacks.

II. LITERATURE SURVEY

TITLE : Decentralized Authentication Using Smart Contracts for Data Retrieval
AUTHOR : H. Chen and J. Li
YEAR : 2023
DESCRIPTION Decentralized Authentication Using Smart Contracts for Data Retrieval" by H. Chen and J. Li (2023) investigates the application of smart contracts in creating a decentralized authentication framework for data retrieval processes. The authors propose a system where users can control their authentication credentials through blockchain technology, eliminating the need for centralized authorities that can be vulnerable to breaches. This model enables secure and automated transactions between users and data providers, ensuring that only authorized individuals can access sensitive information. The paper discusses the advantages of using smart contracts, including transparency, immutability, and reduced reliance on third parties. By embedding authentication logic within the smart contracts, the system can automatically enforce access controls based on predefined criteria, which enhances security and efficiency. The authors also address potential scalability challenges, providing insights into how their approach can be adapted to handle increasing volumes of users and data requests in real-world applications. Overall, this research contributes to the evolving landscape of decentralized systems, promoting greater user autonomy and security in data retrieval scenarios.

TITLE : Privacy-Preserving Authentication Techniques in Cloud Environments
AUTHOR : S. Patel, M. A. Khan, and L. Zhao
YEAR : 2023
DESCRIPTIONPrivacy-Preserving Authentication Techniques in Cloud Environments" by S. Patel, M. A. Khan, and L. Zhao (2023) delves into the critical challenge of securing user identities while maintaining privacy in cloud computing. The authors examine a range of cryptographic methods designed to enhance authentication processes without exposing sensitive personal information during data exchanges. The paper highlights various privacy-preserving techniques, such as zero-knowledge proofs and homomorphic encryption, which allow users to authenticate themselves without revealing their credentials or other identifying information. By utilizing these techniques, the

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

authors demonstrate how cloud services can protect user privacy while ensuring secure access to data. Additionally, the study discusses practical implementations of these methods in real-world cloud environments, analyzing their effectiveness in preventing unauthorized access and data breaches. The authors also explore the balance between usability and security, emphasizing the importance of creating solutions that not only safeguard user data but also maintain a seamless user experience. This research contributes to the ongoing discourse on privacy in cloud computing, providing valuable insights for developers and organizations seeking to enhance security measures in their cloud-based applications.

TITLE : Multi-Factor Authentication Using Biometric and Behavioral Data
AUTHOR : A. Kumar and R. Singh
YEAR : 2022
DESCRIPTION "Multi-Factor Authentication Using Biometric and Behavioral Data" by A. Kumar and R. Singh (2022) explores a comprehensive approach to enhancing security in authentication systems by integrating biometric identifiers and behavioral analytics. The authors argue that traditional password-based authentication methods are increasingly vulnerable to various threats, necessitating the adoption of more robust solutions. In their study, Kumar and Singh detail how combining biometric data—such as fingerprints, facial recognition, and voice patterns—with behavioral metrics—like typing speed, mouse movements, and usage patterns—creates a multi layered defense against unauthorized access. This dual approach not only improves the accuracy of user identification but also provides a dynamic authentication process that adapts to individual user behaviors.

TITLE : User-Centric Data Retrieval: Enhancing Authentication Mechanisms
AUTHOR : Y. Zhang, A. X. Li, and R. J. Wang
YEAR : 2021
DESCRIPTION User-Centric Data Retrieval: Enhancing Authentication Mechanisms" by Y. Zhang, A. X. Li, and R. J. Wang (2021) investigates the intersection of user control and data security in modern authentication frameworks. The authors emphasize the need for a user-centric approach that prioritizes individual privacy while ensuring secure access to sensitive information. The paper presents a novel framework that utilizes blockchain technology to decentralize authentication processes, allowing users to maintain ownership and control over their personal data. By removing reliance on centralized servers, which are often susceptible to breaches, the proposed system enhances data integrity and security. The authors detail the mechanisms through which users can authenticate themselves without compromising their sensitive information, leveraging cryptographic techniques to protect against unauthorized access.

TITLE : Secure and Privacy-Preserving User Authentication for Cloud-Based Services
AUTHOR : M. Alzahrani, Y. Q. Zhang, and N. Kumar
YEAR : 2021
DESCRIPTION This paper addresses the challenges of user authentication in cloud computing environments, focusing on secure and privacy-preserving techniques. The authors propose a new authentication framework that utilizes a combination of cryptographic protocols and multi-factor authentication to protect user credentials while maintaining privacy. They discuss the implementation of zero knowledge proofs and encryption methods that ensure users can verify their identity without exposing sensitive information to cloud service providers. The study also evaluates the performance and usability of the proposed solution, demonstrating its effectiveness in preventing unauthorized access and enhancing user trust in cloud services. By providing a comprehensive analysis of existing approaches and their limitations, the authors contribute valuable insights into the development of more secure and privacy-aware authentication mechanisms for cloud applications.

EXSISTING SYSTEM

- However, the existing work only provides the authentications between users and publishers and suffers from the delay enlargement problem.
- In existing works in-network big-data retrieval leads the network to be seriously vulnerable to a variety of attacks such as malicious-request and data-poisoning attacks.

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712035

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

DRAWBACKS

- Delay-enlargement problem.
- Increasing authentication delays
- Unable to prevent the malicious-request and data-poisoning attacks

PROPOSED SYSTEM

- We design a trust model, namely a suspension-chain model (SCM), which is a trust chain that seamlessly merges certificate authority (CA)-based trust and neighbour-based trust.
- Based on SCM, we propose the DC AUTH integrating certificate collection and packet forwarding, where the suspension certificate chain can be constructed for realizing any authentication to the unpredictable users/IPEs/publishers without accessing servers.

ADVANTAGES

- Providing data-centric authentication
- Reducing authentication delays
- Prevent the malicious-request and data-poisoning attacks

Good Results

SYSTEM ARCHITECTURE

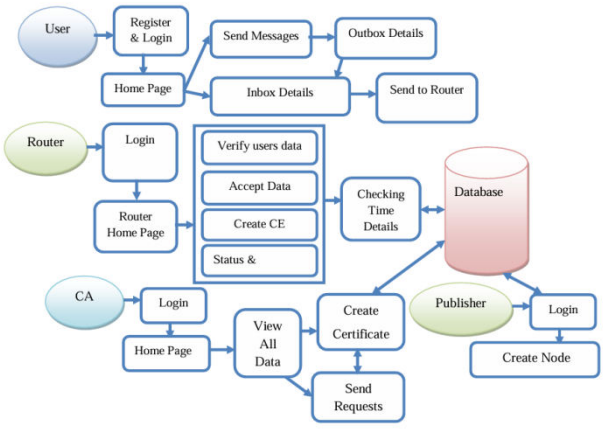

Fig.no:4.2 System Architecture

Figure 1: System Architecture

III. METHODOLOGY

MODULES NAME: This project having the following five modules:

- User Interface Design
- User
- Router
- Certificate Authority
- Publisher

User Interface Design To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.

User This is the second module in our project where User plays the main part of the project role. It are the key functionalities of the User. Enter all details register first all user details are stored in database. User having one account in server based on that user login then Send messages. Then if any users sending any messages it verify and given reply. It verifying inbox and sending outbox messages

Router This is the Third module in our project where router working process. Router has to login with valid username and password. After login successful he can do some operations such as View Accept user requests messages, View users, Exchange certificate, Users feedbacks, and Status of application.

Certificate Authority This is the fourth module in our project where certificate authority process. Certificate authority has to login with valid username and password. After login successful he can do some operations such as View users, Create certificate then verify all details. CA-based trust between two entities is established using the CA as the "introducer." The CA is managed by the network operator, and provides certificates to the owner's entities and the highly trusted physical entities close to them in the HTIG. The entities in the HTIG then confer CA-based trust relationships and issue certificates to each other.

Publisher This is the fifth module in our project where Publisher process. Publisher has to login with valid username and password. After login successful he can do some operations such as Create Nodes.
Publisher: an entity that publishes data in the network.
User: an entity that retrieves data from the network.
Physical entity: an entity that communicates using aphysical device. This could be an IPE or a publisher node (PN) that hosts applications.
Logical entity: an entity that is involved in an application. This can be an authorizer, a sub-authorizer, or a publisher.

IV. IMPLEMENTATION

DEVELOPMENT TOOLS

This chapter is about the software language and the tools used in the development of the project. The platform used here is JAVA. The Primary languages are JAVA, J2EE and J2ME. In this project J2EE is chosen for implementation.

FEATURES OF JAVA

1 THE JAVA FRAMEWORK

Java is a programming language originally developed by James Gosling at Microsystems and released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++ but has a simpler object model and fewer low-level facilities. Java applications are typically compiled to byte code that can run on any Java Virtual Machine (JVM) regardless of computer architecture. Java is general-purpose, concurrent, class-based, and object-oriented, and is specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere". Java is considered by many as one of the most influential programming languages of the 20th century, and is widely used from application software to web applications the java framework is a new platform independent that simplifies application development internet. Java technology's versatility, efficiency, platform portability, and security make it the ideal technology for network computing. From laptops to datacenters, game consoles to scientific supercomputers, cell phones to the Internet, Java is everywhere! 43

2 OBJECTIVES OF JAVA

To see places of Java in Action in our daily life, explore java.com. Why Software Developers Choose Java Java has been tested, refined, extended, and proven by a dedicated community. And numbering more than 6.5 million developers, it's the largest and most active on the planet. With its versatility, efficiency, and portability, Java has become invaluable to developers by enabling them to:

- Write software on one platform and run it on virtually any other platform

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712035

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- Create programs to run within a Web browser and Web services
- Develop server-side applications for online forums, stores, polls, HTML forms processing, and more
- Combine applications or services using the Java language to create highly customized applications or services
- Write powerful and efficient applications for mobile phones, remote processors, low-cost consumer products, and practically any other device with a digital heartbeat Some Ways Software Developers Learn Java Today, many colleges and universities offer courses in programming for the Java platform. In addition, developers can also enhance their Java programming skills by reading Sun's java.sun.com Web site, subscribing to Java technology-focused newsletters, using the Java Tutorial and the New to Java Programming Center, and signing up for Web, virtual, or instructor-led courses. ObjectOriented To be an Object Oriented language, any language must follow at least the four characteristics.

1. Inheritance :It is the process of creating the new classes and using the behavior of the existing classes by extending them just to reuse the existing code and adding addition a features as needed.
2. Encapsulation: It is the mechanism of combining the information and providing the abstraction.
3. Polymorphism: As the name suggest one name multiple form, Polymorphism is the way of providing the different functionality by the functions having the same name based on the signatures of the methods.
4. Dynamic binding: Sometimes we don't have the knowledge of objects about their specific types while writing our code. It is the way of providing the maximum functionality to a program about the specific type at runtime.

3 JAVA SWING OVERVIEW

Abstract Window Toolkit (AWT) is cross-platform Swing[1] provides many controls and widgets to build user interfaces with. Swing class names typically begin with a J such as JButton, JList, JFrame. This is mainly to differentiate them from their AWT counterparts and in general is one-to-one replacements. Swing is built on the concept of Lightweight components vs AWT and SWT's concept of Heavyweight components. The difference between the two is that the Lightweight components are rendered (drawn) using purely Java code, such as drawLine and drawImage, whereas Heavyweight components use the native operating system to render the components. Some components in Swing are actually heavyweight components. The top-level classes and any derived from them are heavyweight as they extend the AWT versions. This is needed because at the root of the UI, the parent windows need to be provided by the OS. These top-level classes include JWindow, JFrame, JDialog and JApplet. All Swing components to be rendered to the screen must be able to trace their way to a root window of one of those classes. 45 Note: It generally it is not a good idea to mix heavyweight components with lightweight components (other than as previously mentioned) as you will encounter layering issues, e.g., a lightweight component that should appear "on top" ends up being obscured by a heavyweight component. The few exceptions to this include using heavyweight components as the root pane and for popup windows. Generally speaking, heavyweight components will render on top of lightweight components and will not be consistent with the look and feel being used in Swing. There are exceptions, but that is an advanced topic. The truly adventurous may want to consider reading this article from Sun on mixing heavyweight and lightweight components.

4 EVOLUTION OF COLLECTION FRAMEWORK: Almost all collections in Java are derived from the java.util.Collection interface. Collection defines the basic parts of all collections. The interface states the add() and remove() methods for adding to and removing from a collection respectively. Also required is the to Array() method, which converts the collection into a simple array of all the elements in the collection. Finally, the contains() method checks if a specified element is in the collection. The Collection interface is a sub interface of java.util.Iterable, so the iterator() method is also provided. All collections have an iterator that goes through all of the elements in the collection. Additionally, Collection is a generic. Any collection can be written to store any class. For example, Collection can hold strings, and the elements from the collection can be used as strings without any casting required. There are three main types of collections:

- Lists: always ordered, may contain duplicates and can be handled the same way as usual arrays
- Sets: cannot contain duplicates and provide random access to their elements
- Maps: connect unique keys with values, provide random access to its keys and may host duplicate values

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712035

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. EXPERIMENTAL RESULTS

1 Home page

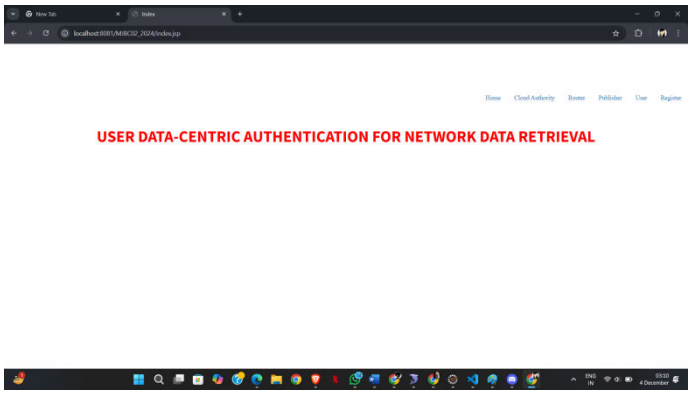

Figure 1:Home Page

The homepage Contains login.

2 User register Page

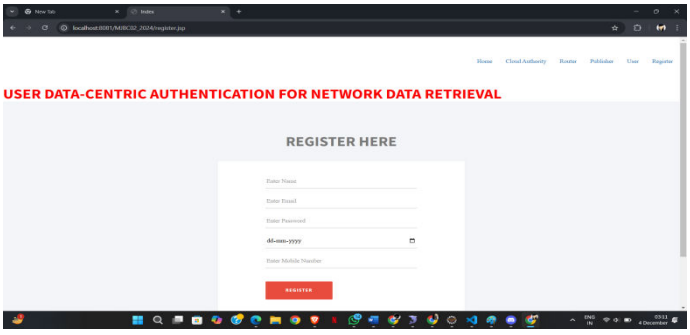

Figure 2User register Page

In this page user has to enter his/her username and password to create login to the account

3 Similar Login's pages

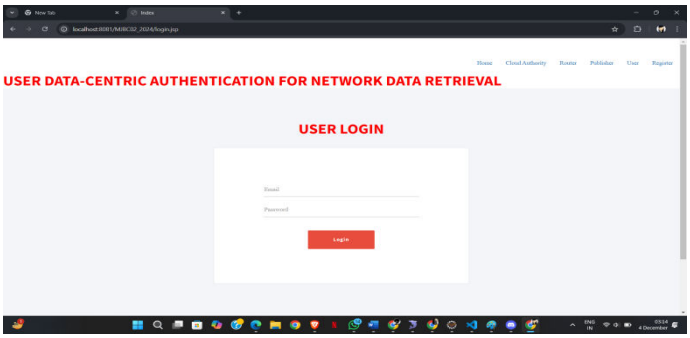

Figure 3.1:User LoginPage

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712035

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

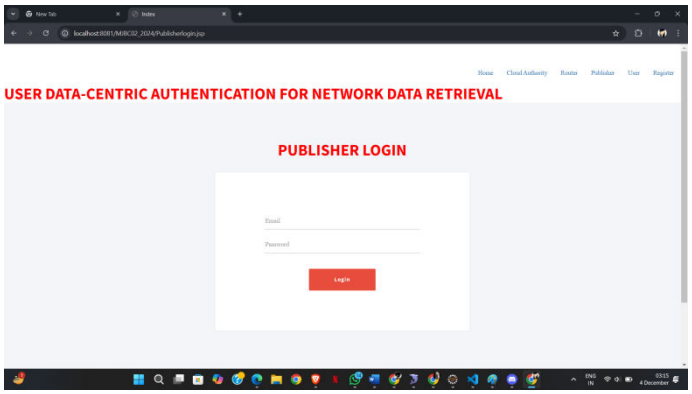

Figure 3.2: Publisher Login page

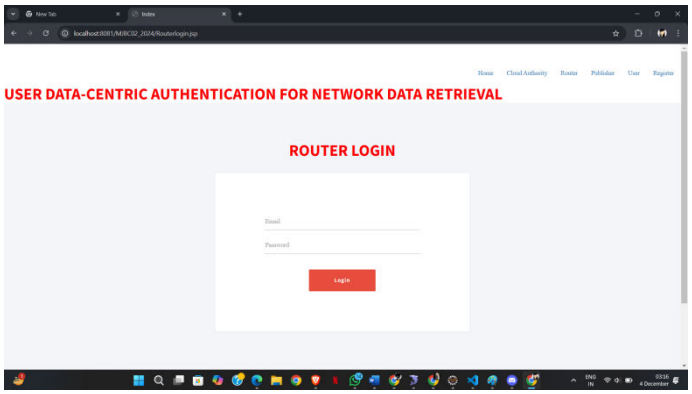

Figure 3.3: Router Login page

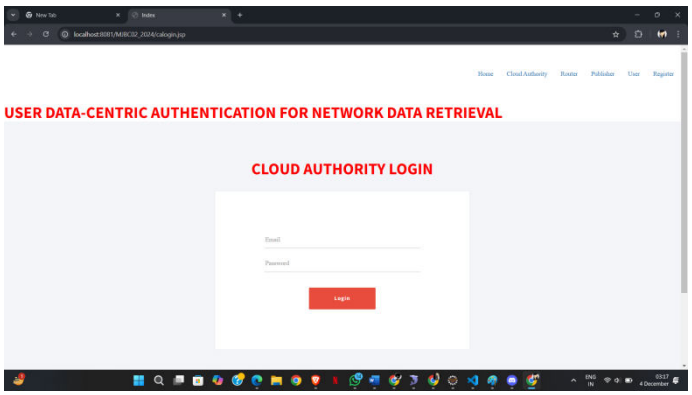

Figure 3.4: Cloud Authority Login page

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712035

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4 Router sequence

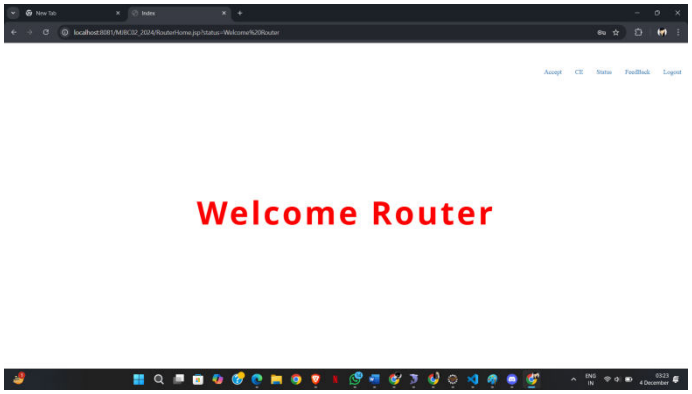

Figure 4.1 : Router Home Screen

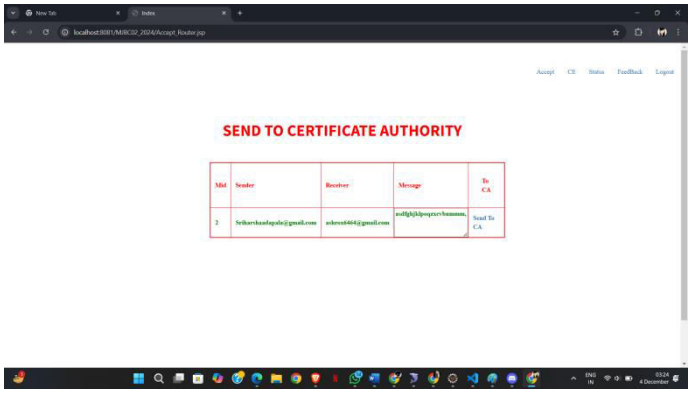

Figure 4.2 : Sending Message to Certify

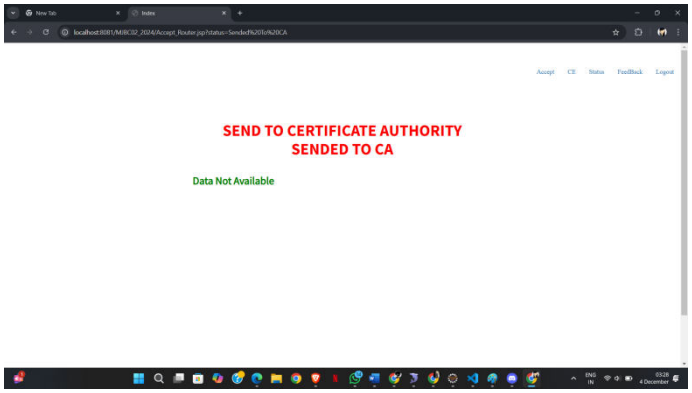

Figure 4.3 : Sent Successfully to CA

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712035

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

5 CA Sequence

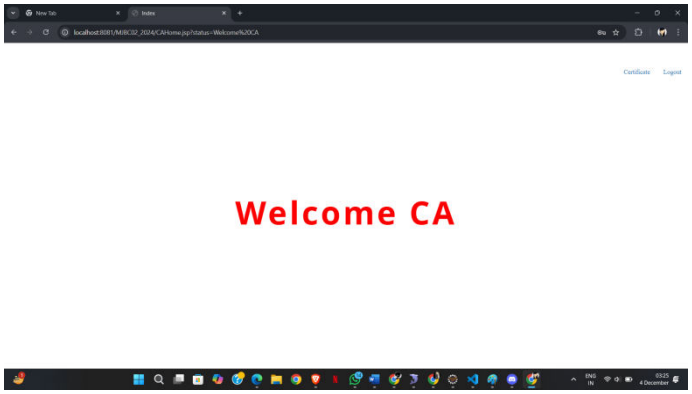

Figure 5.1 : CA Home Screen

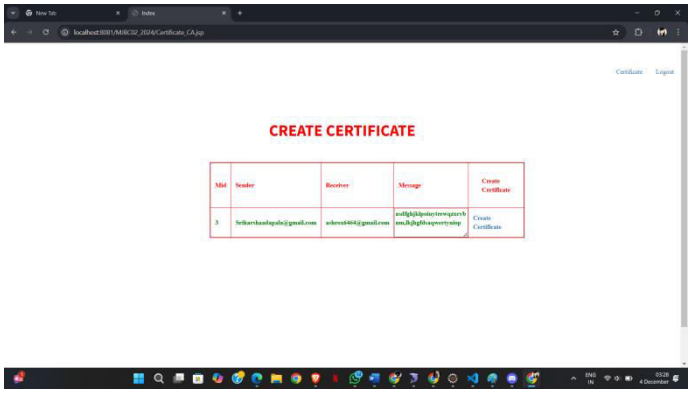

Figure 5.2 : Creating Certification for Message

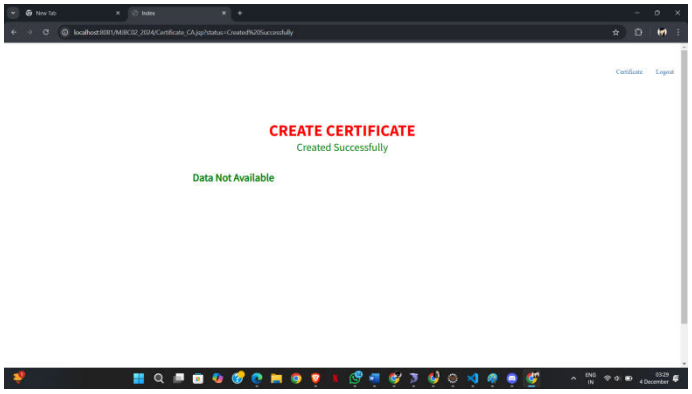

Figure 5.3: Created Successfully

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712035

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

6 Router Sequence return

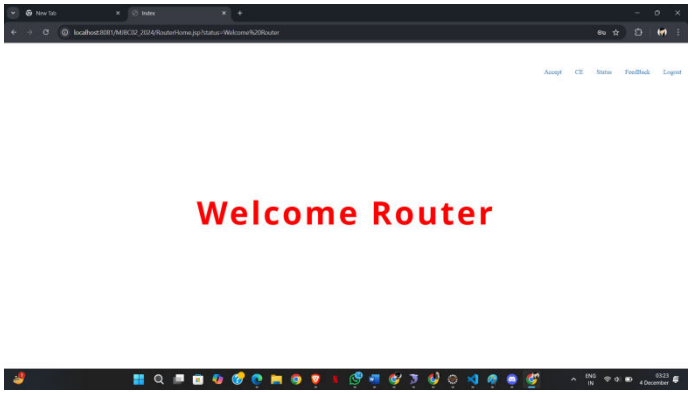

Figure 6.1 Router Home Screen

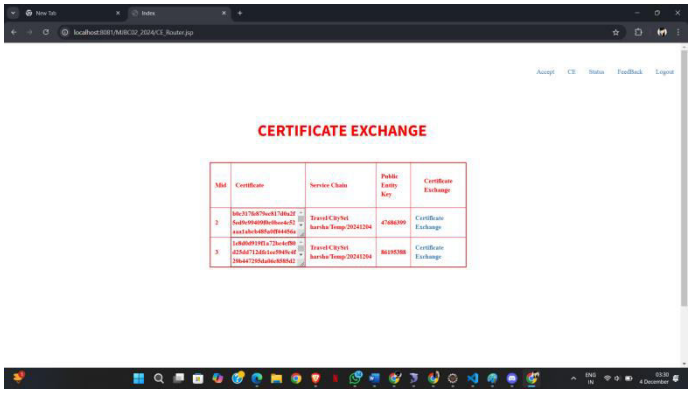

Figure 6.2 : Exchanging Certificate

7 Publisher Sequence

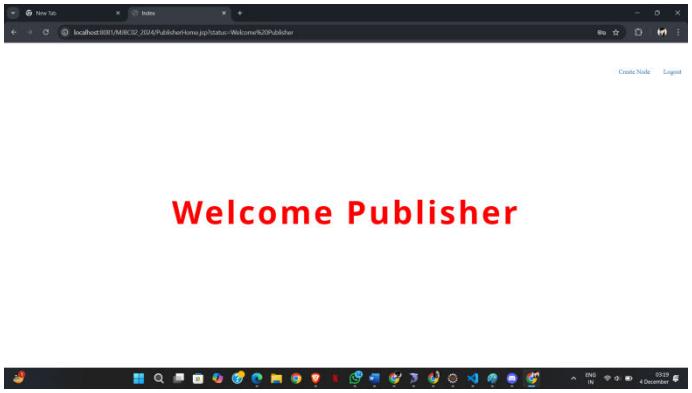

Figure 7.1 : Publisher Home Screen

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712035

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

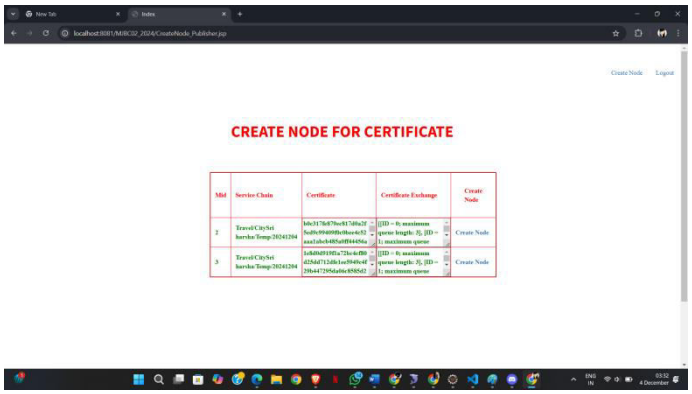

Figure 7.2: Creating Node

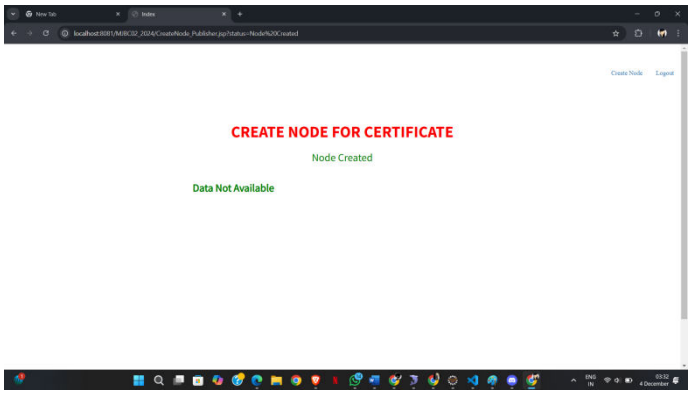

Figure 7.3 Node created Successfully

8 Reciver Inbox

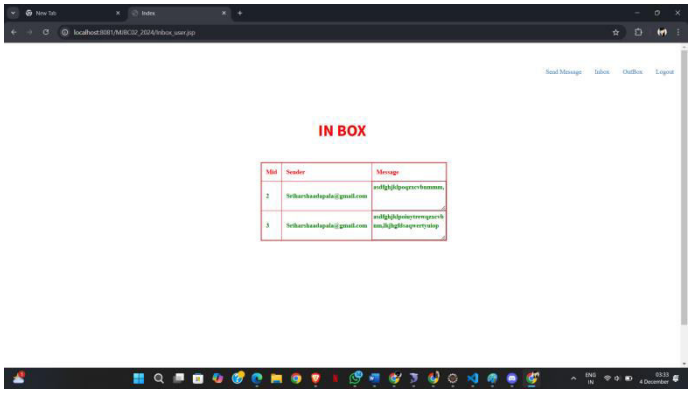

Figure 8: inbox of the message reciver

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. CONCLUSION

In-network big-data retrieval is vulnerable to malicious request and data-poisoning attacks. To prevent such attacks, we proposed DC AUTH, which provides data-centric authentication with merging CA-based trust and neighbour-based trust. It enables authentication among entities including users, IPEs, copy holders, and publishers, regardless of their unpredictability. Extensive simulations have been conducted, and show that DC AUTH can reduce the delay for certificate collection compared to PKI-NDN and can prevent malicious-request and data-poisoning attacks efficiently.

VII. FUTURE ENHANCEMENT

In further detail, the insiders cause slightly more bandwidth consumption than the outsiders. It is because around 10 data retrievals are tolerated to discover malicious-request insiders, and users need to retrieve and authenticate the fake data in order to discover data-poisoning insiders. In contrast, the outsiders can be prevented by the first-hop certificate checks from neighbours, as they do not have valid certificates. Therefore, we see that DC AUTH achieves a minimal additional delay without incurring additional certificate retrievals and its bandwidth consumption is acceptable for performance while efficiently preventing malicious-request and data-poisoning attacks for in-network big-data retrieval.

REFERENCES

[1] N. Khan, I. Yaqoob, I. Hashem, Z. Inayat, W. Ali, M. Alam, M. Shiraz, andA. Gani, “Big Data: Survey, Technologies, Opportunities, and Challenges,”The Scientific World Journal , Vol. 2014, 2014.
[2] H. Yin, Y. Jiang, C. Lin, Y. Luo, and Y. Liu, “Big data: Transforming thedesign philosophy of future Internet,” IEEE Network, vol. 28, no. 4, pp.14-19, July 2014.
[3] S. Yu, and S. Guo (Eds.), “Big Data Concepts, Theories, and Applications,” Springer 2016, ISBN 978-3-319-27761-5.
[4] J. Saltzer, D. Reed, and D. Clark, “End-to-end arguments in systemdesign,” ACM Transactions on Computer Systems, 2 (4), pp. 277-2881984.
[5] S. Yu, M. Liu, W. Dou, X. Liu, and S. Zhou, “Networking for Big Data:A Survey,” IEEE Communications Surveys and Tutorials, Vol. 19, Issue 1,pp. 531-549, 2017.
[6] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman,“A survey of information-centric networking,” IEEE CommunicationsMagazine, 50(7), pp.26-36, 2012.
[7] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S.Shenker, and I. Stoica, “A data-oriented (and beyond) network architecture,” ACM SIGCOMM 2007, Aug. 2007.
[8] P. Jokela, A. Zahemszky, C. E. Rothenberg, S. Arianfar, and P. Nikander,“LIPSIN: Line Speed Publish/Subscribe Inter-Networking,” Proceedingsof the ACM SIGCOMM 2009, pp. 195-206, Aug. 2009.
[9] A. Ghodsi, S. Shenker, T. Koponen, A. Singla, B. Raghavan, and J.Wilcox, “Information centric networking: seeing the forest for the trees,”Proceedings of the 10th ACM Workshop on Hot Topics in Networks, 2011.
[10] S. K. Fayazbakhsh, Y. Lin, A. Tootoonchian, A. Ghodsi, T. Koponen, B.Maggs, K. Ng, V. Sekar, and S. Shenker, “Less pain, most of the gain:incrementally deployable icn,” Proceedings of the ACM SIGCOMM 2013conference, pages 147-158, 2013.
[11] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs,and R. L. Braynard, “Networking named content,” ACM CONEXT’09,Rome, Italy, Dec. 2009.
[12] E. AbdAllah, H. Hassanein, and M. Zulkernine, “A survey of security attacks in information centric networking,” IEEE Communications Surveys& Tutorials, vol. 17, issue 3, 2015. 75
[13] R. Li, and H. Asaeda, “Secure In-Network Big Data Provision with Suspension Chain Model,” IEEE Conference on Computer Communicationsworkshop on BigSecurity 2018, Honolulu, Apr. 2018.
[14] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang,“Interest flooding attack and countermeasures in named data networking,IFIP Networking, pp. 1-9, 2013.
[15] A. Compagno, M. Conti, P. Gasti, and G. Tsudik, “Poseidon: mitigatinginterest flooding ddos attacks in named data networking,” IEEE LCN’13,pp. 630-638, Oct. 2013. [16] T. Nguyen, R. Cogranne, and G. Doyen, “An optimal

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

statistical testfor robust detection against interest flooding attacks in ccn," IFIP/IEEEInternational Symposium on Integrated Network Management (INM), pp.252-260, 2015.
[17] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "Dos and ddos in named datanetworking," In the IEEE ICCCN'13, pages 1-7, July 30-Aug. 2, 2013. [18] C. Ghali, G. Tsudik, and E. Uzun, "Network-layer trust in named-datanetworking," ACM SIGCOMM Computer Communication Review, vol.44, number 5, Oct. 2014.
[19] D. Kim, S. Nam, J. Bi, and I. Yeom, "Efficient content verificationin named data networking," ACM Conference on Information-CentricNetworking, pp. 109-116, 2015.
[20] Z.Su, Y.Hui, Q.Xu, T.Yang, J.Liu, and Y.Jia, "An Edge Caching Schemeto Distribute Content in Vehicular Networks," IEEE Transactions onVehicular Technology, vol. 67, no. 6, June 2018.
[21] Z. Su, Q. Xu, Q.Yang, and F.Hou, "Edge Caching for Layered VideoContents in Mobile Social Networks," IEEE Transactions on Multimedia,vol. 19, no. 10, pp. 2210-2221, 2017.
[22] L. Gu, D. Zeng, S. Guo, Y. Xiang, and J. Hu, "A General CommunicationCost Optimization Framework for Big Data Stream Processing in Geodistributed Data Centers," IEEE Transactions on Computers, vol. 65, no.1, pp. 19-29, Jan. 2016.
[23] J. Wu, S. Guo, J. Li, and D. Zeng, "Big Data Meet Green Challenges:Big Data towards Green Applications," IEEE Systems Journal, vol. 10, no.3, pp. 888-900, Sept. 2016.
[24] J. Wu, S. Guo, H. Huang, W. Liu, and Y. Xiang, "Information andCommunications Technologies for Sustainable Development Goals: Stateof-the-Art," IEEE Communications Surveys & Tutorials, vol. PP, no. 99,DOI: 10.1109/COMST.2018.2812301, 2018.
[25] S. Yu, "Big Privacy: Challenges and Opportunities of Privacy Study inthe Age of Big Data," IEEE Access, Vol. 4, pp. 2751-2763, 2016. 76
[26] R. Li, H. Asaeda, J. Li, and X. Fu, "A Verifiable and Flexible DataSharing Mechanism for Information-Centric IoT," IEEE InternationalConference on Communications (ICC 2017), Paris, France, May 2017.
[27] S. Yu, G. Wang, and W. Zhou, "Modeling Malicious Activities in CyberSpace," IEEE Network, Vol. 29, Issue 6, 2015.
[28] R. Li, H. Asaeda, and J. Li, "A Distributed Publisher-Driven Secure DataSharing Scheme for Information-Centric IoT," IEEE Internet of ThingsJournal, vol. 4, issue 3, pp. 791-803, June 2017.
[29] S. Yu, S. Guo, and I. Stojmenovic, "Fool Me If You Can: Mimicking Attacks and Anti-attacks in Cyberspace," IEEE Transactions on Computers,Vol. 64 Issue 1, pp.139-151, 2015.
[30] H. Lu, J. Li, and M. Guizani, "Secure and Efficient Data Transmission forCluster-based Wireless Sensor Networks," IEEE Transactions on Paralleland Distributed Systems, Vol. 25 Issue 3, pp.750-761, 2014. [31] K. Wang, J. Yu, X. Liu, and S. Guo, "A Pre-Authentication Approachto Proxy Re-encryption in Big Data Context," IEEE Transactions on BigData. (accepted)
[32] Q.Xu, Z.Su, Q.Zheng, M.Luo, and B.Dong, "Secure Content Deliverywith Edge Nodes to Save Caching Resources for Mobile Users in GreenCities," IEEE Transactions on Industry Informatics, vol. 14, issue 6, June2018.
[33] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "DiscriminatingDDoS Attacks from Flash Crowds Using Flow Correlation Coefficient,"IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp.1037-1080, June 2012.
[34] A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hua, and S. Guo, "Protection of Big Data Privacy," IEEE Access, vol. 4, pp. 1821-1834, Apr.2016.
[35] K. Hamedani, L. Liu, R. Atat, J. Wu, and Y. Yi, "Reservoir ComputingMeets Smart Grids: Attack Detection Using Delayed Feedback Networks,"IEEE Trans. Industrial Informatics, vol. 14, no. 2, pp. 734-743, 2018.
[36] T. Dierks, and E. Rescorla, "The transport layer security (TLS) protocol,"IETF RFC 5246, Aug. 2008.
[37] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R Housley, and WPolk, "Internet X.509 public key infrastructure certificate and certificaterevocation list (CRL) prole," IETF RFC 5280, May 2008. 77
[38] P. Hoffman and J. Schlyter, "The DNS-based authentication of nameentities (DANE) transport layer security (TLS) protocol: TLSA," IETFRFC 6698, Aug. 2012.
[39] D. Basin, C. Cremers, T. Kim, A. Perrig, R. Sasse, and P. Szalachowski,"Design, Analysis, and Implementation of ARPKI: an Attack-ResilientPublic-Key Infrastructure," IEEE Transactions on Dependable and SecureComputing (TDSC), DOI: 10.1109/TDSC.2016.2601610, 2016.
[40] P. Zimmermann, "The official PGP user's guide," MIT Press, 1995.
[41] N. Li, W. H. Winsborough, and J. C. Mitchell, "Distributed credentialchain discovery in trust management," Journal of Computer Security, vol.11, no. 1, pp. 35-86, Feb. 2003.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[42] K. Hamouid, and K. Adi, "Self-certified based trust establishment schemein ad-hoc networks," 2012 5th International Conference on New Technologies, Mobility and Security (NTMS), Turkey, May 7-10, 2012.
[43] S. Capkun, L. Buttya, and J.-P. Hubaux, "Self-organized public-keymanagement for mobile ad hoc networks," IEEE Transactions on MobileComputing, vol. 2, issue 1, pp. 52-64, 2003.
[44] A. Ulrich, R. Holz, P. Hauck, and G. Carle, "Investigating the OpenPGPweb of trust," The 16th European conference on Research in computersecurity, pp. 489-507, Sept. 2011.
[45] Y. Yu, "Public key management in named data networking," NDNTechnical Report, NDN 0029, 2015.
[46] A. Afanasyev, "Addressing operational challenges in named data networking through NDNS distributed database," PhD thesis, UCLA, 2013.
[47] A. Hoque, S. Amin, A. Alyyan, B. Zhang, L. Zhang, and L. Wang,"NLSR: named-data link state routing protocol," The 3rd ACM SIGCOMM workshop on Information-centric networking, pp. 15-20, 2013.
[48] A. Ghodsi, T. Koponen, J. Rajahalme, P. Sarolahti, and S. Shenker,"Naming in content oriented architectures," The 1st ACM SIGCOMMworkshop Information-centric networking, Aug. 2011.
[49] A. Afanasyev, I. Moiseenko, and L. Zhang, "ndnSIM: NDN simulator for NS-3," NDN Technical Report, NDN-0005, http://nameddata.net/techreports.html, 2012.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com