International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST229211

Using Zero-Knowledge Proof for Secure Data Transmission on Distributed Network

E. Jansirani [1], Dr. N. Kowsalya [2]
[1]Computer Science, Lowry Memorial College, Bangalore, India
[2]Computer Science, Sri Vijay Vidhyalaya College of Arts and Science, Nallampalli, Dharmapuri, India

Article Info
Volume 9, Issue 2
Page Number : 75-80

Publication Issue
March-April-2022

Article History
Accepted : 10 March 2022
Published : 20 March 2022

ABSTRACT

Data security plays a major role in computer network. Because it helps to transmit data in secure way over the Internet. So we need to use strong security method for secure data transaction. Cryptography is a security tool which helps to transmit information from one place to another place over computer network. Cryptography follows encryption and decryption methods for data transmission. Cryptographic technique is completely based on key generation because it needs keys to transmit data between users. However cryptography works well in secure data transmission but it needs keys to provide security for data. In cryptography generation of keys taking more time than transmission of data. So in this paper we discuss about Zero-Knowledge Proof (ZKP) which is also based on cryptographic technique. ZKP is also useful in secure data transmission without sharing key values between users. This paper tells about overview of ZKP and how it is useful in data transmission.

Keywords : ZKP, Prover, Verifier, Secret

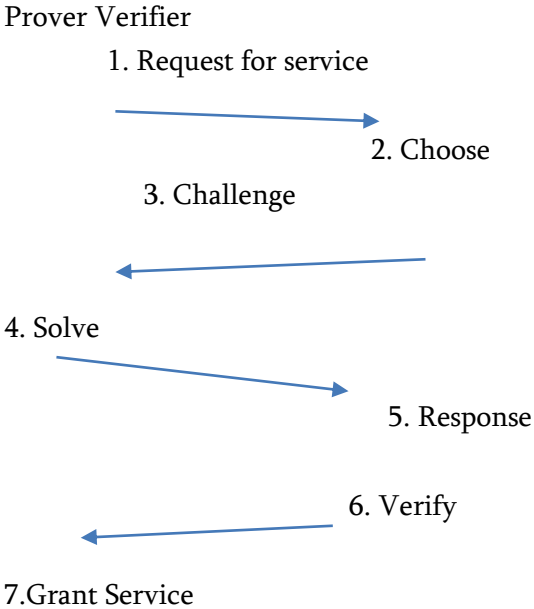
I. INTRODUCTION

Zero-Knowledge Proof is introduced by Glodwasser, Micali and Rackoff in 1989.Zero-Kowledge Proof is the most beautiful and powerful concept in computer science. ZKP is completely based on mathematical functions and equations. ZKP provides best way of authenticating users because it does not allow users to share any password between them, when we do not reveal any secret before transmission then no one can find what kind of information is being transmitted between sender and receiver and what kind of files has been transmitted. The term "Zero Knowledge" is formed with no (Zero) information (Knowledge) should be revealed during communication. Zero-Knowledge Proof is the two-way protocol between sender and receiver for data communication.

II. HOW DOES ZKP WORK?

In Zero-Knowledge Proof the person who is going send information is known as prover and the person who is going to receive information is known as verifier. ZKP always tells that the prover has to prove

his identity before transmission and the verifier has to verify the prover's identity. After verifying the identity the verifier allows the prover to send the data. Zero-Knowledge Proof is an encryption scheme and based on technique where one party can prove the truthful information to another party. The following diagram describes about how ZKP proof verifies and accepts the communication between users.



1. Request for service: This is the first phase for making communication between users, in this phase the person who wish to transmit information they can send request message to the verifier.

2. Choose: This is the second phase which will always happen in the verifier's side, here the list of provers will be waiting in this state. The verifier has to choose the user for transmission of data, here users no need to wait for longer time.

3. Challenge: Once the user has been chosen by the verifier then the verifier has to challenge the prover that he is valid user or not.

4. Solve: This task will always happen on prover's side. Prover has to compute the value according to the question which is given by the verifier.

5. Response: After calculating the value response will be sent to the verifier the one who is going to check the value.

6. Verify: Once the value received from the prover, the verifier has to post the value in zero knowledge proof algorithm to check the value

7. Grant Service: If the algorithm gives the positive value then the prover is valid user so communication will be taken place. If the algorithm gives the negative value then the prover is not a valid user so the communication will not be taken place.

ZKP builds the secure channel between users to provide protection during data exchange. When others use tight hacking technique to steal data it protects in such a way that it avoids data leakage in any tight hacking method. This is the safest technique in transfer of sensitive information because it supports powerful authentication method.

III. TYPES OF ZERO KNOWLEDGE PROOF

The scenario of zero knowledge proof tells about it is possible to make communication with two parities in such a way without sharing or without revealing it. Based on this Zero Knowledge Proof has divided into two main categories.

i) Interactive Zero Knowledge Proof
ii) Non-interactive Zero Knowledge Proof

A. Interactive Zero Knowledge Proof:

In this type of ZKP needs interaction between users for each and every transaction. This method tells the person who is going to send information they have to compute the value and have to prove to sender that he is the valid user. The person takes N number of times to compute the value to satisfy the verifier. Interactive Zero Knowledge proof is completely based on the value which is sent by verifier. If the verifier accepts the prover is valid user then the message has been transferred them. If the verifier found that the user is not valid one then the verifier will not accept the communication with the prover. The following steps explain the concept of interactive ZKP:

Step 1: Receive the value from the verifier

Step 2: Perform computation with the value taken from the verifier

Step 3: Send the computed value to the verifier

Interactive ZKP follows the mentioned three steps to identity whether the user is valid or invalid. Here always the communication will begin with a challenge of the verifier and the response by the prover. The following is an example of interactive Zero Knowledge Proof:

1.User A picks random value k in the given range k= 1……n

2.User A computes the value of $h=g^k \bmod p$, here g is an auto generator and p can be a prime number and sends to User B

3.User B picks random value q1 in the given range q1=1…..n and sends to User A

4.User A computes the value v1=i(q1)+k mod n and sends to User B

5.User B puts this value to interactive zero knowledge protocol to verify the user

6.This protocol returns value either 1 or 0

7.If it is 1 the user will be considered to be a valid user and communication will be taken place

8.It it is 0 the user is called as a cheater and no communication will be allowed

However interactive zero knowledge proof does not allow fake communication between users. There are two main drawbacks in interactive ZKP, the first one verification will be taken place for every transaction this will take more time and emergency situation the message will get delivered late due to this verification. The second one during interactive ZKP both the users need to be in online until the communication terminated, in case of poor network the communication will not resume instead it will begin from the first step.

B.Non-interactive Zero Knowledge Proof

In this type of zero knowledge proof user who is going to communication with other user they both need not to talk or communicate during data transmission. Non interactive zero knowledge proof system always having only messages between prover and verifier. This type completely focused to avoid interaction for sending message between users, here common reference string will be given to all the users who wish to transmit data using non interactive ZKP. The person who wish to transmit data they can transmit data along with the reference string, then the person (verifier) who is going to receive they can see the message if the message has the common string then the message will be acceptable or the message get denied by the person. The question will come to our mind is if malicious user or fraud user gets this common string then they can also send wrong message to the verifier. To avoid this kind of confusion this non interactive ZKP gives random string to each and every user. Once the string has been used that never get repeated to any user for data transmission. So, malicious user tries to use this string the receiver will get alerted and that kind of communication will not be entertained in this method. We can transmit information with one reference string at a time and the string cannot be used for next data transmission.

How does non-interactive zero knowledge work?

Step 1: User A has the information to be sent which is known as secret S

Step 2: User A sends the secret message along with common reference string known as P

Step 3: User B receives the message P from User A

Step 4: User B divides the received message such that original message and common string

Step 5: If the common reference string is valid string then the message will be accepted by User B or else the received message will be ignored by User B

The main issue faced by all users in non-interactive zero knowledge is using common reference string. This string has the bound limit of sending message. Bound limit tells about the size of message, within

that limit we have to combine original message and common string. If cheater knows the common string then he will play your role like all message will be sent to verifier as you sent.

IV. PROPERTIES OF ZERO KNOWLEDGE PROOF

The following are properties of ZKP:

Completeness: If the statement is true then the prover is a honest user so the communication will be taken place

Soundness: If the statement is false then the prover is a cheater so the communication will not be taken place

Zero Knowledge: If the statement is true the prover need not reveal any information rather than message wants to transfer

V. ADVANTAGES OF ZERO KNOWLEDGE PROOF

Simplicity: Zero Knowledge Proof does not require any complicated encryption method because this method is not going to reveal any information to end users. ZKP is completely focused on secure data transmission and it does not support any kind of key exchange so, ZKP is very simple for secure data transmission

Privacy: Zero Knowledge Proof does not allow any user to share personal information or data. So here user details will be kept confidential. Complete privacy will be achieved in using ZKP

Security: It strengthens security by using effective authentication methods. The authentication mechanism used in ZKP provides complete protection for user's data because malicious user will not break this authentication method so our data will be transferred in secure way

Scalability: ZKP allows to add or remove any number of users on network. So, number of users will not affect the protection mechanism in ZKP. Whenever we add or remove users in ZKP the originality of authentication method will not change or get affected by other users in network

VI DISTRIBUTED NETWORK

This one type of network which helps to combine and deliver data from more than one network. Distributed network is completely based on server and client machines, all communication on distributed network will go via server machine. Here server machine will be having details about authorized users on network. According to their usage permission rights will be given to each user on distributed network. We know that in distributed system all the nodes are connected with one another. Adding or removing number of nodes can be easier in distributed network. Failure of a single node does not affect the entire network and with the help of other nodes we can continue communication. Resources such as printers and scanners can be kept as common and these resources can be shared effectively by all the users on network

VI. CONCLUSION

ZKP is security tool which provides secure data transmission over the network. It is completely based on cryptographic technique. In cryptography communication is totally depend on keys. There are two types of keys supported by cryptography public key and private key. Cryptography allows data transmission only after successful transmission of keys. Key generation time will be more than the data transmission time. Keeping this in mind ZKP has been developed to save time during data transmission. In ZKP user can only post their value for data transmission the value will be computed by ZKP protocol. Distributed network is a collection of node connected with one another. The main disadvantage in distributed network is to provide adequate security to each and every user on network, when we combine distributed network along with ZKP we can achieve both fast data transmission and security for data. Another problem in distributed network is loss of data, to avoid this ZKP has two types they are

interactive ZKP and non-interactive ZKP. In interactive ZKP each transaction will be having the proof from receiver so there will be less chance of losing information. If we go with next type here the common string helps to avoid losing of data because without knowing the string the communication will not be taken place. So, I conclude that ZKP will help to stop loss of data as well as providing security for data in distributed network in efficient way.

VII. REFERENCES

[1]. S. Goldwasser, S. Micali, and C. Rackoff, "Knowledge complexity of interactive proof systems," SIAM Journal on Computing, vol. 18, no. 1, pp. 186–208, 1989.

[2]. M. Blum, P. Feldman, and S. Micali, "Non-interactive zero-knowledge and its applications," in Proceedings of the 20th Annual ACM symposium on Theory of computing (STOC '88), pp. 103–112, ACM, 1988

[3]. M. Blum, A. de Santis, S. Micali, and G. Persiano, "Noninteractive zero-knowledge," SIAM Journal on Computing, vol. 20, no. 6, pp. 1084–1118, 1991.

[4]. S. Bayer, J. Groth, and editors, "Efficient zero knowledge argument for correctness of a shuffle," in Advances in Cryptology—EUROCRYPT 2012, D. Pointcheval and T. Johansson, Eds., vol. 7237 of Lecture Notes in Computer Science, pp. 263–280, Springer, 2012.

[5]. J. Groth, "Simulation-sound NIZK proofs for a practical language and constant size group signatures," in Advances in Cryptology—ASIACRYPT 2006, X. Lai and K. Chen, Eds., vol. 4284 of Lecture Notes in Computer Science, pp. 444–459, Springer, 2006.

[6]. Zero-knowledge proofs of identity U Feige, A Fiat, A Shamir - Journal of cryptology, 1988 – Springer

[7]. Noninteractive statistical zero-knowledge proofs for lattice problems C Peikert, V Vaikuntanathan - Annual International Cryptology Conference, 2008 – Springer

[8]. Toward Non-interactive Zero-Knowledge Proofs for NP from LWE RD Rothblum, A Sealfon, K Sotiraki - Journal of cryptology, 2021 – Springer

[9]. Feige U, Lapidot D, Shamir A. Multiple non-interactive zero knowledge proofs random string. Proceedings of the 31st Annual Symposium on Foundations of Computer Science (SFCS '90); 1990; pp. 308–317.

[10]. Damgård I. Non-interactive circuit based proofs and non-interactive perfect zero-knowledge with proprocessing. In: Rueppel RA, editor. Advances in Cryptology—EUROCRYPT '92. Vol. 658. Springer; 1993. pp. 341–355. (Lecture Notes in Computer Science)

[11]. Fortnow L. The complexity of perfect zero-knowledge. Proceedings of the 19th annual ACM symposium on Theory of computing (STOC '87); 1987; ACM; pp. 204–209

[12]. Damgård I, Thorbek R. Non-interactive proofs for integer multiplication. In: Naor M, editor. Advances in Cryptology—EUROCRYPT 2007. Vol. 4515. Springer; 2007. pp. 412–429. (Lecture Notes in Computer Science)

[13]. On the complexity of distributed network decomposition A Panconesi, A Srinivasan - Journal of Algorithms, 1996 - Elsevier

[14]. Distributed network protocols A Segall - IEEE transactions on Information Theory, 1983 - ieeexplore.ieee.org

[15]. Interactive physical zero-knowledge proof for Norinori JG Dumas, P Lafourcade, D Miyahara, T Mizuki… - International Computing …, 2019 – Springer

[16]. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems O Goldreich, S Micali, A Wigderson - Journal of the ACM (JACM), 1991 - dl.acm.org

[17]. Privacy preserving authentication system based on non-interactive zero knowledge proof suitable for Internet of Things AD Dwivedi, R Singh, U

Ghosh, RR Mukkamala… - Journal of Ambient …, 2021 - Springer

[18].AN INTERACTIVE ZERO-KNOWLEDGE PROOF BASED PROTOCOL OF IDENTIFICATION AND DIGITAL SIGNATURE [J] M XU, C CHEN, J YING - Journal of Computer Research and …, 2002 - en.cnki.com.cn

[19].Zero-knowledge from secure multiparty computation Y Ishai, E Kushilevitz, R Ostrovsky… - Proceedings of the thirty …, 2007 - dl.acm.org

[20].Interactive hashing can simplify zero-knowledge protocol design without computational assumptions IB Damgård - Annual International Cryptology Conference, 1993 - Springer

[21].Goldreich, O., and H. Krawczyk, On the Composition of Zero-Knowledge Proof Systems, Proc. 17th ICALP, Lecture Notes in Computer Science, Vol. 443, Springer-Verlag, Berlin, 1990, pp. 268–282.

[22].A. de Santis, G. di Crescenzo, and G. Persiano, “Non-interactive zero-knowledge: a low-randomness characterization of NP,” in Automata, Languages and Programming, J. Wiedermann, P. van Emde Boas, and M. Nielsen, Eds., vol. 1644 of Lecture Notes in Computer Science, pp. 271–280, Springer, 1999.

[23].M. Bellare and S. Goldwasser, “New paradigms for digital signatures and mes-sage authentication based on non-interative zero knowledge proofs,” in Advances in Cryptology—CRYPTO '89 Proceedings, G. Brassard, Ed., vol. 435 of Lecture Notes in Computer Science, pp. 194–211, Springer, 1989.

[24].D. F. Ciocan and S. Vadhan, “Interactive and noninteractive zero in the help model,” Cryptology ePrint Archive Report 2007/389, 2007, http://eprint.iacr.org.

Cite this article as :

E. Jansirani, Dr. N. Kowsalya, "Using Zero-Knowledge Proof for Secure Data Transmission on Distributed Network", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 9 Issue 2, pp. 75-80, March-April 2022. Available at doi : https://doi.org/10.32628/IJSRST229211

Journal URL : https://ijsrst.com/IJSRST229211