Paper ID: MISS21_26

Study and Investigation of Pki Based Blockchain Infrastructure

Rashmi Deshmukh*, Shital Gaikwad

Department of Technology, Shivaji University, Kolhapur

Department of Computer Science, Shivaji University, Kolhapur

*Corresponding author

Abstract

Background: PKI is a Public-key Infrastructure that provides secured communication between client and server. The digital certificate gives protection to the user data and communicates securely with a server. But the drawback of PKI is that this certificate issuing authority is given to another website called CA. If the CA systems are attacked by an unsecured system, then this problem cannot be solved easily. These drawbacks of centralized handling of certificate authorities by PKI can be handled by Block chain.

Objectives: To study different PKI based Block chain architectures. To analyse and investigate more robust and faster architecture for secured digital information.

Methodology: We have studied Block chain architecture in detail. Block chain architecture uses distributed DB by maintaining data in the form of blocks. This architecture is secured as a large set of computers are working parallel. Distributed DB is maintained by blockchain for storing Personal Identifiable Information. These are stored with a distributed hash table. With blockchain, the client and server maintain their public key and decentralized identifier on a distributed public ledger. With a public key, any peer node can access the information. Blockchain records digital information and distributes it and is not easily allowed to update.

Results and discussion: Paper [1] gives a robust PKI based on blockchain framework to solve the problem of single point of failure problem with traditional PKI. Solution is given with two methods as log based PKI schema and web of trust. Paper [2] presents an extension field for X.509 certificate and gives the details of peer node with revocation of the certificate.

Conclusions and future work: Block chain is an inventive technology that enables information to be shared without third parties and without transaction costs. Blockchains are able to back up the data read, prevent MITM attacks, and minimize the power of third parties. This protects information in a secure and distributed manner. Hence emerging approach to PKI is the use of blockchain technology in connection with modern cryptocurrencies.

References

[1] Alexander Yakubov, W. S. (April 2018). A Blockchain-Based PKI Management Framework. *IEEE/IFIP man2block 2018At: .* Taipei, Taiwan: 10.1109/NOMS.2018.8406325.

[2] Yves Christian, E. A. (2021). A blockchain-based certificate revocation management and status verification system. *Computers and Security ,Volume 104*.

 DOI: 10.21467/abstracts.120

ISBN: 978-81-954993-2-8