A Blockchain based Security Information and Event Monitoring Framework

Satyanarayana N, Chitresh G

e-Security *Department, Centre for Development of Advanced Computing, Hyderabad, India*

nanduris@cdac.in, chitreshg@cdac.in

Abstract*—Security Information and Event Monitoring (SIEM) tools collect log data which helps organizations to plan appropriate security assessment and reconciliation strategies. The majority of the SIEM tools generate reports instantaneously. Root cause analysis of security risks needs data provenance capabilities. Blockchain Technology augments SIEM tools with data provenance capability so that an effective security framework can be built for organizations. In this paper, we describe a unified and comprehensive security assurance framework which supports a tamper-proof, time-stamped and distributed storage repository to ensure data provenance and is useful in security assessment in compliance to cloud control matrix of CSA. This framework can be used in a Cloud environment also by adding additional security log data collection points.

Keyword— Blockchain, Security Assurance Policy, Continuous Monitoring

N Satyanarayana is a Master of Technology in Computer Science holder from Jawaharlal Nehru Technological University, Hyderabad, India. Prior to this, he completed his Master's in Computer Applications from Sri Venkateswara University in the year 1999. He published several papers in National and International conferences in various areas such as Peer to Peer Computing, Network Management, e-Learning and Blockchain. His current research interest include Blockchain consensus algorithms and reference architectures.