Forensic Attribution in NoSQL Databases

Submitted by grigby1 on Mon, 03/05/2018 - 1:03pm

Title	Forensic Attribution in NoSQL Databases
Publication Type	Conference Paper
Year of Publication	2017
Authors	Hauger, W. K., Olivier, M. S.
Conference Name	2017 Information Security for South Africa (ISSA)
ISBN Number	978-1-5386-0545-5
Keywords	Access Control, attribute-based encryption, authentication, authorisation, cloud computing, cloud implementations, Collaboration, database forensics, forensic attribution, Forensics, Human Behavior, human factors, message authentication, NoSQL, NoSQL databases, Peer-to-peer computing, policy-based governance, pubcrawl, Scalability, Security by Default, security of data, sensitive information, Structured Query Language, survey

Abstract

NoSQL databases have gained a lot of popularity over the last few years. They are now used in many new system implementations that work with vast amounts of data. This data will typically also include sensitive information that needs to be secured. NoSQL databases are also underlying a number of cloud implementations which are increasingly being used to store sensitive information by various organisations. This has made NoSQL databases a new target for hackers and other state sponsored actors. Forensic examinations of compromised systems will need to be conducted to determine what exactly transpired and who was responsible. This paper examines specifically if NoSQL databases have security features that leave relevant traces so that accurate forensic attribution can be conducted. The seeming lack of default security measures such as access control and logging has prompted this examination. A survey into the top ranked NoSQL databases was conducted to establish what authentication and authorisation features are available. Additionally the provided logging mechanisms were also examined since access control without any auditing would not aid forensic attribution tremendously. Some of the surveyed NoSQL databases do not provide adequate access control mechanisms and logging features that leave relevant traces to allow forensic attribution to be done using those. The other surveyed NoSQL databases did provide adequate mechanisms and logging traces for forensic attribution, but they are not enabled or configured by default. This means that in many cases they might not be available, leading to insufficient information to perform accurate forensic attribution even on those databases.

URL	http://ieeexplore.ieee.org/document/8251777/
DOI	10.1109/ISSA.2017.8251777
Citation Key	hauger_forensic_2017

Access Control attribute-based encryption authentication authorisation Cloud Computing cloud implementations collaboration database forensics forensic attribution Forensics Human behavior Human Factors message authentication NoSQL NoSQL databases Peer-to-peer computing policy-based governance pubcrawl Scalability Security by Default security of data sensitive information Structured Query Language survey