

#34



Block Formation for Storing Data on Information Security Incidents for Digital Investigations

Miloslavskaya N. (ngmiloslavskaya@mephi.ru), Nikiforov A., Plakhsy K. NRNU MEPhI, Moscow, Russia,



First Author



Second Author



Third Author

ABSTRACT

Nowadays technologies such as Blockchain (BC) and the Internet of Things (IoT) can be heard everywhere. But because of the leap in the development of these technologies, there is a need to evaluate the existing approaches critically. One of the up-to-date tasks is to study information security (IS) incidents as a part of the IoT. Due to a large number of different manufacturers and options for technology implementation, it cannot be unambiguously concluded what choice will be better. The paper examines the related work in the area and proposes an approach to form the basis for storing data on IS incidents. For this purpose, the authors formulate a block structure for including in a chain for later use, for example, in computer forensics.

INTRODUCTION

In case of incidents investigation in information systems, information security (IS) specialists have a wide range of tools and techniques for data extracting and analysis. But new methods require optimization for modern data scales. Therefore, today researchers are engaged in optimizing solutions, which are not suitable for solving, for example, Big Data problems, for several reasons. New technologies like the BC and the IoT appear for this purpose. The goal of this research was to form a block structure, which would allow data on IS incidents in the IoT to be stored for subsequent use in digital investigations. The following tasks were solved to achieve this goal: to analyze related work in the selected field, to consider the block format in the chain, and to offer a convenient and safe recording format from the viewpoint of storing IS incident data.

BLOCKCHAIN

Since the advent of the Internet, Blockchain technology (BT) has been recognized as one of the most explosive innovations of the beginning of the 21st century. Gartner included it in the 2017 Top 10 strategic technological trends. BT is currently used in financial activities for payments, currency exchange, money transfers, markets, investments, brokerage, insurance, etc., as well as in non-financial applications (e.g., certification systems, development, electronic voting, managing patient records, the IoT, etc.). It is noted that due to its properties to ensure data integrity, as well as various numerous checks, this technology can become one of the most important tools for auditors. The BC in this paper refers to the definition: "a special type of protected distributed data structure (a database) that maintains an expanding list of non-editable blocks/records and sets rules for working with transactions/events recorded in blocks and tied in such a way to them without a central administrator and centralized data storage (unlike regular databases where rules are often set for the entire database and applications)." Such a database is shared by a group of users — nodes — entities in the BC network (transport level of the BC platform) that receive and process transactions and share information about a potential transaction. The node either proves (public BC) or verifies (hybrid/private BC) transactions and then adds them to the block with a unique hash code. Thus, there are two special types stand out among the nodes: miners and validators. Miners look for new transactions in the system (in the corresponding data sources if more precisely) and using cryptographic transformations prove that the transaction is real (valid) for its inclusion in the BC as part of new blocks using evidence such as proof of work/resource/state/activity, etc. Validators check series or individual transactions based on appropriate means of checking. In this paper, the main attention of the technology review is on validators. In this study, the BC, namely a private registry with closed access, is a convenient means of storing IS events in a network environment since it records and arranges them in strictly chronological order. Thus, the BC can be considered as a unidirectional data structure (chain) with a linked list of blocks, each of which refers to the previous one using hash code-pointers stored in the block header. One block with a unique identifier and a "cryptographic" link to the previous valid block combines transactions — IS events belonging to the same IS incident (as its successive steps). Creating a repeating block (its contents is similar to one of the previous blocks) with a new identifier means the presence of repeating events in the network, characteristic, for example, of a Denial-of-Service (DoS) attack.

INTERNET OF THINGS

Today the IoT is increasingly filling up both business and everyday life. The IoT can be observed in cars, houses (Smart Home), hospitals, cities (Smart City), and so on. Many devices constantly receive data for further processing according to a huge number of criteria and analysis to solve a huge number of tasks. An important place on the IoT is occupied by information-gathering sensors (about the urban environment, human health, equipment status) — pressure, humidity, light, movement, heat flow, condition, etc. Thanks to wireless communication and various protocols, they can interact with each other and send the collected data for subsequent analysis by a person or artificial intelligence. Data centers, cloud technologies, and Big Data are used to store and process the received data. Unfortunately, the IoT still does not have a single standard or protocol, which could be adopted as the best solution for everyone. Therefore, each manufacturer chooses for himself the criteria of the system, as well as the methods of data transfer and storage. An important IoT feature is the transparent conditions for working in surrounding networks, which prevents the monopoly of individual corporations — manufacturers of devices. As a result, the concept seeks accessibility and comprehensibility for the whole society without exception. Cooperation between developers, convenient integration of devices and standards and protocols development lead the community to what the IoT is ideally supposed to be used for the best interaction with a person and his health, the best options for solving problems based on available resources and real-time data from open sources, and the best synchronization of service providers and goods with the global capabilities of society as a whole.

HASHING

For the initial verification of IS incidents, the authors propose the use of hashing. It refers to a conversion carried out by a hash function, which is a function that maps strings of bits to fixed-length strings of bits, and it is difficult to calculate the initial data displayed in this value for a given function value, other input data displayed in the same function value for given input data, and any pair of input data mapped to the same value. When applying this method, several variants of hashing algorithms are considered to provide freedom of choice for the experiment implementation. Sending messages with data in the form of hash codes makes it difficult to access them. The presence of the same equipment on the IoT network nodes allows hashing at the verification point without requesting extraneous data, which allows increasing the quality of the verification performed. When an attacker receives a hash code, there will be a problem in selecting a hashing algorithm and decrypting the contents of the message. Comparing to transferring open data to the cloud from network devices, as it is currently accepted on the IoT, it is safer. In the course of the study, several options for hashing algorithms were considered.

BLOCK STRUCTURE

The main attention in this study is given to the contradiction that there is no common base when transmitting data to the cloud from IoT devices, where data on IS events would be brought in and which would be independent of the cloud. Such a database will be useful in case of an IS incident because it allows accessing the history of the IoT infrastructure immediately, without a request to the cloud until it will not be required. It is proposed to use a distributed registry or, in other words, BT to create such a database. This database will not require centralized storage servers, which can be hacked or disconnected from the network as the database is simultaneously stored on all nodes of the infrastructure. As soon as one of the nodes forms and adds a block with data, the remaining nodes learn about it. Therefore, if the database is unavailable on one node, access to information will still be possible due to access from other points of the network. The database will be convenient because it supports the integrity of entered data due to the BT features.

CONCLUSIONS

The authors examined the BC concept and proposed to use BT together with hashing to form an unchanged database of devices and systems, which can be used further in the digital investigation of IoT IS incidents, for example, in computer forensics. An idea of creating a database, the entities in which will be trusted and easy to use, was applied. A block structure that allows storing data on IoT devices and systems for future detailed digital investigations was proposed. Based on the related work's analysis, the necessary fields of the block were determined, and the need for each of them was justified.

ACKNOWLEDGMENTS & REFERENCES

This work was supported by the MEPhI Academic Excellence Project (agreement with the Ministry of Education and Science of the Russian Federation of August 27, 2013, project no. 02.a03.21.0005) and by the Russian Foundation for Basic Research (project no. 18-07-00088).