Blockchain for Wearable IoT Forensics

Justin Wasser

University of Maryland Global Campus

ITEC 650: Computer Forensics

Professor Robinson

10/24/2023

Abstract

Wearable Internet of Things (IoT) devices, due to their dynamic and dispersed architecture, present many challenges to every level of the practice of digital forensics, which necessarily includes the practice of evidence integrity preservation. To that point, a main challenge to the preservation of evidence originating from wearable IoT devices is establishing/documenting a secure and reliable chain of custody for acquired evidence. However, implementing blockchain technology for the practice of wearable IoT forensics offers a potential framework that would resolve the chain of custody issue, thereby improving the processes related to evidence integrity preservation for wearable IoT devices.

Introduction

The following research paper will contain a brief overview of digital forensics with a focus on the processes used to ensure that acquired evidence maintains its integrity, and why that is important to the practice of digital forensics. Next, an examination of how the Internet of Things (IoT), specifically IoT wearables, poses new challenges to digital forensics will be conducted, in addition to why the issues presented are likely to become more relevant in the near future. Lastly, an analysis of blockchain technology will be conducted, with a focus on how its application to the field of IoT forensics will create an improved framework for conducting wearable IoT forensic investigations by providing improved chain of custody capabilities.

To begin, digital forensic investigations are comprised of five distinct phases, which are defined as the "identification, acquisition, preservation, analysis, and subsequent reporting of digital evidence" (Robinson, 2023). However, for the purposes of this paper, we will be focusing on the preservation aspect of the digital forensics framework. To that point, preservation refers to the integrity of an acquired piece of digital evidence, meaning that to preserve a piece of digital evidence for use in court proceedings, its integrity must be maintained throughout the investigative lifecycle (Stoyanova et al., 2020). In traditional digital forensics maintaining the integrity of evidence is relatively straightforward, i.e., a chain of custody document is created detailing all relevant information regarding the acquisition, analysis, and handling of evidence, and subsequently, all acquired digital evidence is hashed using one (or multiple) hashing algorithms which produce a unique value that is then attached to a piece of evidence (*Session 3: Digital Forensics Investigations*, 2023; *Session 4: Data Acquisition I & II*, 2023). Moreover, the hash produced from a forensic image of an original piece of evidence is compared to the hash

value of the original piece of evidence, and if they are identical then the integrity of the imaged piece of digital evidence has been preserved (*Session 3: Digital Forensics Investigations*, 2023).

Wearable IoT devices present new challenges

There is a need for an accepted framework governing forensic investigations (including evidence preservation) involving wearable IoT devices as these devices contain a host of potentially probative information about their users that may be leveraged during investigations (Sakshi et al., 2023). With that said the issue of preserving the integrity of digital evidence becomes more difficult when dealing with digital evidence originating from wearable Internet of Things (IoT) devices (Sakshi et al., 2023). Although there are numerous challenges associated with every aspect of the digital forensic framework when evidence originates from IoT devices, for this paper, we will only be dealing with the challenges regarding the preservation of evidence's integrity (Stoyanova et al., 2020). Therefore, in order to discuss how to go about solving the issue of preserving IoT-based evidence's integrity, it is important to first illuminate the underlying architecture of the IoT. Furthermore, the architecture of the IoT will only be reviewed briefly to facilitate a better understanding of the challenges it presents to the task of preserving the integrity of digital evidence. To that point, IoT architecture is similar to cloud-based architecture as IoT devices process information and relay it via networks to various cloud systems (Stoyanova et al., 2020). However, unlike conventional cloud-connected devices (computers), wearable IoT devices are much smaller and therefore often lack the hardware to store significant amounts of data locally (Atlam et al., 2020).

Moreover, wearable IoT devices are likely to encounter many different networks as they are mobile devices traveling with their user (Stoyanova et al., 2020). Therefore, pieces of digital evidence may be dispersed across many different sources and analysis will require piecing

together multiple pieces of evidence to create evidence of probative value (Stoyanova et al., 2020). However, as previously mentioned, for evidence to be admissible in court its integrity must be demonstrated (likely several times), a large part of which relies on a documented chain of custody (*Session 4: Data Acquisition I & II*, 2023). As a result, creating and maintaining a chain of custody ledger for the many different sources of digital evidence associated with wearable IoT devices proves to be extremely challenging due to the dynamic nature of the IoT environment (Stoyanova et al., 2020). Lastly, this issue is only going to increase in importance as wearable IoT devices continue to proliferate, as exemplified by a projected "compound annual growth rate of 19.48 percent between 2020 and 2026" (Sakshi et al., 2023) for wearable IoT devices (Sakshi et al., 2023).

Unlike in traditional digital forensics, it is very unlikely that most relevant evidence will be located at the device level with wearable IoT devices due to their limited hardware, therefore network and cloud forensics will play a larger role in wearable IoT forensic investigations compared to traditional digital forensics (Atlam et al., 2020). Therefore, many of the major issues associated with IoT forensics overlap with issues that face cloud forensics, i.e. a lack of standardization among cloud providers, multitenancy, jurisdictional limitations, and a lack of visibility into where data may be physically located (*Session 10: Analysis, Email, Cloud and Validation*, 2023; Stoyanova et al., 2020). Furthermore, these challenges make demonstrating the integrity of forensic images of original evidence more difficult because in some instances it may not be possible to obtain the hardware containing the original source of evidence due to one or more of the reasons just listed (*Session 10: Analysis, Email, Cloud and Validation*, 2023; Stoyanova et al., 2020).

Additionally, these challenges have led to there not being an accepted methodology for preserving the integrity of digital evidence collected during IoT forensic investigations (Atlam et al., 2020). Furthermore, because "The **completeness** and **accuracy** of digital evidence collection is often question [sic] in the legal arena" (*Session 10: Analysis, Email, Cloud and Validation*, 2023) there is a significant need for a framework that supports chain of custody-related documentation for wearable IoT forensic investigations (Atlam et al., 2020). To that point, blockchain technology appears to have the characteristics necessary to provide that much-needed framework (Sakshi et al., 2023).

Blockchain technology as a solution

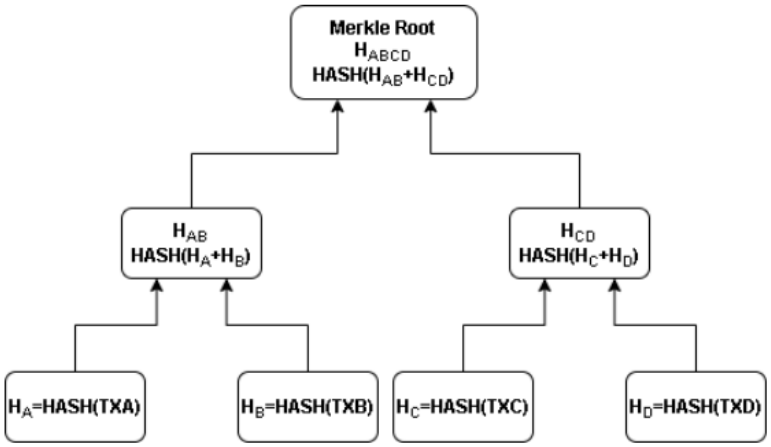
One possible solution to many of the challenges associated with preserving the integrity of evidence collected from wearable IoT devices is the use of blockchain technology (Sakshi et al., 2023). To that point, blockchain technology facilitates the creation of a "decentralized database" (Sakshi et al., 2023) of linked transactions/data that are "linked to the previous one through cryptographic hashes" (Sakshi et al., 2023) which functionally produces a distributed permanent record of data that is sufficiently resistant to unauthorized attempts to alter it (Sakshi et al., 2023). Furthermore, this method for creating a secure record can be leveraged to establish a trustworthy chain of custody archive for acquired evidence in wearable IoT forensics (Sakshi et al., 2023). Therefore, a further analysis of blockchain technology's architecture is required at this time.

For starters, several pieces of important information are contained within each block stored on a blockchain, with each block constituting a transaction/event in the overall ledger (Mahrous et al., 2021). In the context of a wearable IoT forensic investigation, these pieces of information include all information found on a traditional chain of custody document such as

identifying information about a given IoT device, what type of acquisition was performed on the device, when the acquisition was performed, using which tool, and who performed the acquisition (Sakshi et al., 2023). Moreover, this information is stored efficiently via the creation of the block's Merkle "root hash" (Mahrous et al., 2021). Furthermore, additional information such as the previous block's hash value, the block's timestamp, and the "nonce" (Mahrous et al., 2021) associated with a given block is also stored within a block (Mahrous et al., 2021).

The nonce of a given block is used to add additional randomness to the block's composition, ensuring that the hash calculated for a given block is unique, i.e. no two blocks have the same hash output (Gulen, 2022). While the block's timestamp serves as documentation of when a given block in a blockchain was generated (Sakshi et al., 2023). Additionally, a Merkle tree is constructed within a given block utilizing the hashes created for pieces of evidence and related forensic activities (Mahrous et al., 2021). More specifically the Merkle tree utilizes the hashes of all forensic events/activities within the single block being constructed and combines two of those event hashes at a time until there is only one hash remaining (Mahrous et al., 2021). Furthermore, the final hash consisting of the combined hashes of all pieces of evidence and related forensic activities constituting a single forensic event/activity is known as the Merkle "root hash" (Sakshi et al., 2023). The architecture of the described Merkle tree is illustrated in Figure 1.

Figure 1: Merkle tree architecture



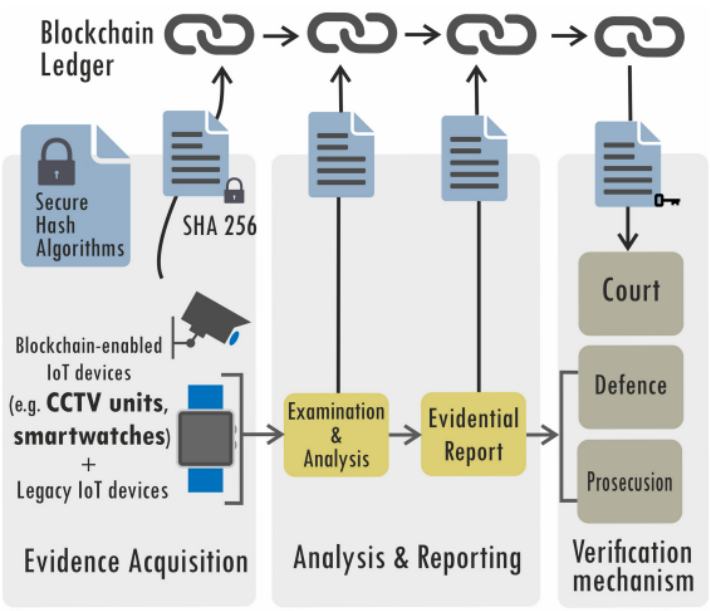
(Mahrous et al., 2021)

Next, an additional hash value is created based on the inclusion of both the root hash of a block combined with the hash of the previous block in the blockchain which is known as a "block header" (A S, 2023). This means that checking the root hash of a given block and validating its integrity also serves to "validate the transactions across all blocks" (Mahrous et al., 2021). By requiring as part of the algorithm used for calculating every new block's hash the hash output of the block directly preceding a linking of events occurs (Mahrous et al., 2021; Sakshi et al., 2023). Moreover, this makes the entire blockchain resistant to unauthorized modification attempts as the Merkle root hash will be altered if any previous block is tampered with (Mahrous et al., 2021; Sakshi et al., 2023). In practice, this helps resolve a vulnerability presented by a centralized chain of custody, where only a single actor is needed to alter or destroy evidence (Sakshi et al., 2023).

Beyond blocks, blockchain technology also requires the use of "smart contracts" (Mahrous et al., 2021). To that point, a "smart contract" (O'Dowd et al., n.d.) governs what level of access to information housed on a blockchain different parties are granted, and it also governs

who and under what conditions a party may add a transaction (or in this case piece of evidence or related activity) to the blockchain (O'Dowd et al., n.d.). To that point, once a transaction has been deemed valid it will be added to the blockchain ledger allowing other parties to view the transaction/evidentiary item (O'Dowd et al., n.d.). In this instance, a transaction would occur whenever a new event occurred that requires documenting as part of the chain of custody for a specific case i.e., events involving the "seizure, custody, control, relocation, analysis and disposition of evidence" (*Session 4: Data Acquisition I & II*, 2023). Therefore, blockchain technology is well suited to meet chain of custody-related requirements as smart contracts can be written specifically for cases involving wearable IoT forensic investigations, granting appropriate privileges and access to the various parties involved (Mahrous et al., 2021). The described wearable IoT forensic blockchain chain of custody architecture is illustrated in Figure 2.

Figure 2: Blockchain-enabled chain of custody



(Stoyanova et al., 2020)

Furthermore, employing blockchain technology on a dedicated network to establish a chain of custody for wearable IoT-related evidence provides numerous benefits including, making the chain of custody record sufficiently resistant to attacks that seek to destroy the integrity of evidence as "stored information cannot be modified without consensus from all participants" (Sakshi et al., 2023). Furthermore, the blockchain-enabled forensic framework provides "immutability and audibility, which are critical characteristics of a DF chain of evidence" (Mahrous et al., 2021). This is crucial in the field of digital forensics as potential evidence must withstand legal scrutiny from opposing counsel and/or expert witness(es) to be admitted as evidence in court proceedings. To that point, prosecutors and/or expert witness(es) will not be able to successfully challenge the use of blockchain technology for chain of custody documentation as it meets many if not all of the admissibility considerations used when evaluating forensic evidence across the various standards (Rule 702, Daubert, and Frye) used by courts across the united states (*Forensic Evidence Admissibility & Expert Witnesses*, n.d.).

Lastly, one of the major standards includes whether the technology in question has achieved "general acceptance" (*Forensic Evidence Admissibility & Expert Witnesses: Daubert Standard*, n.d.), which blockchain technology certainly has. Therefore, blockchain technology provides a framework that allows evidence acquired from wearable IoT devices to meet the chain of custody record requirements necessary for said evidence to be deemed admissible in court proceedings (Sakshi et al., 2023).

Conclusion

In conclusion, wearable IoT devices present a myriad of challenges to the field of digital forensics due to their dynamic and dispersed architecture, and the percentage of digital forensic cases utilizing evidence originating from wearable IoT devices is likely to grow in the near

future (Sakshi et al., 2023; Stoyanova et al., 2020). Furthermore, one of the main challenges in this environment is the establishment of a chain of custody for evidence acquired from wearable IoT devices and their supporting infrastructure (Stoyanova et al., 2020). However, blockchain technology, especially due to its underlying use of Merkle trees, has the necessary characteristics to provide a secure and reliable chain of custody for evidence acquired during wearable IoT forensic investigations (Sakshi et al., 2023). Furthermore, events that may be securely recorded via blockchain technology are not limited to only data collected from wearable IoT devices as periphery information such as information about the acquisition tool used, the examiner(s) performing the acquisition, and other such information may also be stored within the IoT forensic blockchain (Sakshi et al., 2023). Finally, the use of blockchain technology for recording chain of custody-related transactions/events regarding wearable IoT evidence allows for simple and continuous testing of the integrity of stored evidence so that said evidence will be deemed admissible during court proceedings (Mahrous et al., 2021).

Bibliography

A S, R. (2023, January 17). *Merkle Tree in Blockchain: What is it and How does it work | Simplilearn*. Simplilearn.com. https://www.simplilearn.com/tutorials/blockchain-tutorial/merkle-tree-in-blockchain

Atlam, H. F., El-Din Hemdan, E., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2020). Internet of Things Forensics: A Review. *Internet of Things*, *11*, 100220. https://doi.org/10.1016/j.iot.2020.100220

Forensic Evidence Admissibility & Expert Witnesses. (n.d.). Www.forensicsciencesimplified.org. Retrieved October 23, 2023, from https://www.forensicsciencesimplified.org/legal/index.htm

Forensic Evidence Admissibility & Expert Witnesses: Daubert Standard. (n.d.). Www.forensicsciencesimplified.org. Retrieved October 23, 2023, from https://www.forensicsciencesimplified.org/legal/daubert.html

Gulen, K. (2022, December 22). *Blockchain Nonce Explained: What Is It And How It Operates?* Dataconomy. https://dataconomy.com/2022/12/15/blockchain-nonce-explained/#:~:text=What%20is%20nonce%20in%20blockchain

Mahrous, W. A., Farouk, M., & Darwish, S. M. (2021). An Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hash. *IEEE Access*, *9*, 151327–151336. https://doi.org/10.1109/access.2021.3126715

O'Dowd, A., Bradley, M., & Lucas, M. (n.d.). *What is blockchain?* Www.ibm.com. Retrieved October 23, 2023, from https://www.ibm.com/cloud/architecture/architectures/blockchainArchitecture/overview

Robinson, M. (2023, August 19). *A few thoughts of my own...* Learn.umgc. https://learn.umgc.edu/d2l/le/920316/discussions/threads/28929695/View

Sakshi, Malik, A., & Sharma, A. K. (2023). Blockchain-based digital chain of custody multimedia evidence preservation framework for internet-of-things. *Journal of Information Security and Applications*, *77*, 103579. https://doi.org/10.1016/j.jisa.2023.103579

Session 3: Digital Forensics Investigations. (2023). Learn.umgc. https://learn.umgc.edu/d2l/le/content/920316/Home

Session 4: Data Acquisition I & II. (2023). Learn.umgc. https://learn.umgc.edu/d2l/le/content/920316/Home

Session 10: Analysis, Email, Cloud and Validation. (2023). Learn.umgc. https://learn.umgc.edu/d2l/le/content/920316/Home

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191–1221. https://doi.org/10.1109/comst.2019.2962586