STM JOURNALS

Journal of
Advanced Database
Management & Systems

ISSN: 2393-8730
Volume 11, Issue 1, 2024
January—April
DOI (Journal): 10.37591/JoADMS

https://journals.stmjournals.com/joadms

Review JoADMS

Security of Cloud Computing from a Blockchain Perspective

Vatsal K. Bhuva*

Abstract

Originally, the foundation of the Internet was trust. There are increased threats and problems after many information disclosures. We have employed even more modern Internet-based devices in recent years. Among the primary issues raised in literature, privacy, data protection, and trust require particular consideration. In this case, a new paradigm for information security has arisen, one that is built on transparency rather than the closed, cryptic methods used in present models. Recently, certain projects utilising Blockchain technology and techniques have emerged. The aim of this work is to construct a preliminary version of the model based on our preliminary research, which is referred to as systematic mapping in the methodology. We provide an overview of several Blockchain-based Internet of Things (IoT) platforms, models, strategies, and other projects. We also assess each paper's compliance with 11 essential IoT requirements. This work adds to the growing corpus of knowledge in the fields of trust, privacy, and security. Our results are helpful for businesses from a variety of industries that are a part of the Internet ecosystem as well as for further research at the Academy. They can profit from the combined knowledge and use it as a guide to define their development methods that are focused on the new IoT paradigms.

Keywords: Blockchain, cloud computing, Internet of Things, IoT, ontology, privacy, security

INTRODUCTION

Devices connected to the Internet of Things (IoT) produce, handle, and share enormous volumes of privacy-sensitive data as well as security-critical data; as a result, they are popular targets for many types of cyberattacks [1]. Many of the modern networkable devices that make up the Internet of Things are lightweight and low power. The majority of these devices' processing power and energy must be dedicated to carrying out essential application functions, which makes it difficult to provide security and privacy on a budget. Conventional security techniques are typically costly for IoT in terms of processing overhead and energy usage. Furthermore, because of their high degree of centralization, scale challenges, many-to-one nature of communications, and single point of failure, many modern security frameworks are not well suited for the Internet of Things [2].

*Author for Correspondence
Vatsal K. Bhuva
E-mail: vatsal.kailash@gmail.com

Student, Department of Cloud Computing, Conestoga College, Cambridge, Ontario, Canada

Received Date: January 17, 2024
Accepted Date: February 07, 2024
Published Date: April 03, 2024

Citation: Vatsal K. Bhuva. Security of Cloud Computing from a Blockchain Perspective. Journal of Advanced Database Management & Systems. 2024; 11(1): 7–11p.

Current approaches to safeguard user privacy frequently either expose noisy or insufficient data, which could make it more difficult for some IoT applications to provide customised services [3]. As a result, IoT requires a distributed, lightweight, and scalable security and privacy solution. Due to its distributed, private, and secure characteristics, the Blockchain (BC) technology, which powers Bitcoin, the original cryptocurrency system [4], has the ability to overcome the aforementioned difficulties. One application domain that unifies

various technological and societal fields is the Internet of Things (IoT). IoT research is diverse, but its definition is still up for debate [1].

In this regard, a new method for ensuring the security and openness of information has emerged. It replaces the closed, cryptic methods used in the present information security models. Blockchain technologies and methodologies have been proposed by some initiatives [2].

One of the main challenges in developing IoT-based devices or embedded systems is the lack of a modelling architecture, language, or formalism that facilitates the cohesive development and integration of the many Semantic Web Stack disciplines. We have challenges: on top of complexity and scalability, we also have time latency issues (the Bitcoin network takes 10 min at the moment) and a high number of confirmations needed for transactions, which goes against IoT notions of real-time processing [1]. Every node in the Bitcoin network can see every transaction. This poses some challenges (i.e., transactions executed for a limited number of network nodes) when we require devices for regulated environments [3].

Understanding how traditional software development could be modified or improved to meet the new Blockchain-based Internet of Things requirements is crucial in this context.

What is consolidated information about the factors influencing the development of devices?

We are undertaking a methodical mapping of crucial elements in embedded systems' construction based on IoT paradigms in order to accomplish the study's objective. We are seeking responses to the following queries in this study: (i) Is blockchain-based Internet of Things built to withstand development processes? Furthermore, (ii) what attributes, tenets, or prerequisites of blockchain-based IoTs have been taken into account in blockchain-based IoT development processes?

Understanding Blockchain-based IoT domains and industry best practices, as well as presenting the most recent findings about device (or thing) construction, are the primary goals of this research. Furthermore, this endeavour adds to the relatively young and continuously expanding understanding of the Internet of Things' security, privacy, and trust-aspects that are yet mostly unexplored. This work is helpful for academic research in the future as well as for businesses from a variety of industries that are involved in the Internet ecosystem. These businesses stand to gain from the combined knowledge and can use it as a roadmap to define their development methods that are tailored to the new IoT paradigms.

THE BLOCKCHAIN OVERVIEW

At the heart of many decentralized financial systems, including Bitcoin and others, is a universal digital ledger called the Blockchain. Every transaction made by participants is documented on the blockchain, with data privacy and operational verification ensured through cryptographic techniques. Every transaction is verified by multiple participants, resulting in extremely redundant verification. In exchange for their computing labour, they receive rewards [5].

Organizations utilizing blockchain technology stand to gain transparency, democracy, decentralization, security, and efficiency. Financial services can be accessed via Blockchain, which also offers the main benefits of the conventional correspondent banking system: (1) uniform process standards; and (2) longer-term worldwide reconnaissance.

The Blockchain Ontology

The Blockchain Ontology with Dynamic Extensibility, or BLONDIE, ontology is the first attempt to standardise this technology. This OWL ontology enables the representation of specific aspects of the Ethereum or Bitcoin frameworks in RDF format. It can be expanded to include additional Blockchain technologies as well. Furthermore, as OWL, BLONDIE has the capacity to provide explicit knowledge [3].

According to Ugarte *et al.*, the best-case scenario would be for everyone to adopt forks with little to no change or the original Bitcoin technology [6]. Although Bitcoin has many limits and was not intended for use for purposes other than financial transactions, the protocol itself is already standardized and well-defined, thus this is not a feasible situation. We need to concentrate our efforts on addressing the interoperability between Blockchain systems, which is currently one of the most talked-about concerns in the Blockchain community. Direct communication between the gadgets would allow them to address issues, update software, and keep an eye on energy consumption [7].

RESEARCH METHODOLOGY

The four steps of the research technique were separated. Only Step #2 (Systematic Mapping), which is depicted in Figure 1 and is explained in depth below, will be covered in this study.

Risks and Security Concerns with Cloud Computing

Seven security concerns were identified by Gartner in 2008 [8], and they must be addressed before enterprises fully adopt the cloud computing concept.

- *Data location:* Some clients may not be aware of the precise location of their data when it is stored on cloud servers.
- *Regulatory compliance:* Clients have the option of selecting providers who agree to be audited by outside agencies that verify the security measures offered by cloud service providers.
- *Data segregation:* Since encrypted data from several organizations may be kept in one location, a system that divides data from several organizations is necessary and ought to be supplied by the cloud service provider.
- *Long-term viability:* This refers to the capacity to revoke an agreement and all data in the event that the present provider is acquired by a different company.

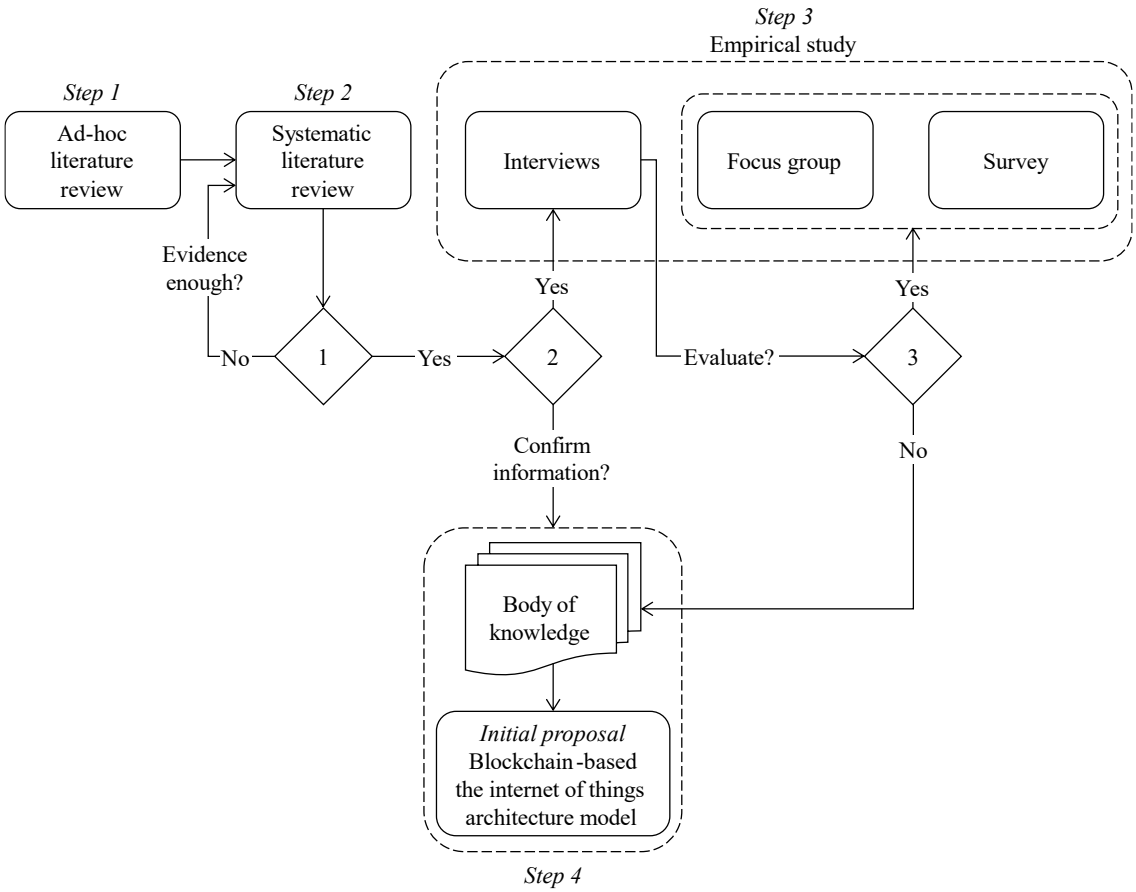

Figure 1. Scientific methodology steps [9].

CURRENT TRENDS AND CHALLENGES

This section outlines the key themes and obstacles explored by authors in the papers regarding Blockchain-based IoT.

Skarmeta *et al.* highlighted that vulnerabilities within IoT systems can result in various security breaches, including but not limited to, malicious breaches compromising confidentiality and authentication, clandestine assaults compromising service integrity, or disruptions to network availability like DoS attacks [4]. Additionally, privacy and anonymity are significant concerns. IoT devices inherently gather and disseminate data, posing distinct challenges to personal privacy.

Specifically, the difficulties encompass the widespread engagement of users with intelligent entities and collections of objects, alongside the unregulated accumulation of this data on opaque platforms. This situation potentially exposes users to various risks, including but not limited to, identification, pinpointing, surveillance, tracking, manipulation, profiling, targeted marketing, data association, and even social manipulation.

Buchmann explored the primary factors influencing the levels of integrity, anonymity, and adaptability within the blockchain [10]. Additionally, he recommended a deeper examination of the security features offered by Proof of Work, which has traditionally played a pivotal role in enabling distributed consensus.

The Ethereum platform facilitates the implementation of transaction processing rules or scripts via smart contracts. Some authors conducted research into the security implications of executing smart contracts on Ethereum within an openly distributed network [6, 11]. They identified numerous emerging security issues, indicating nuanced deficiencies in comprehending the distributed semantics of the platform. These researchers advocate for augmenting operational semantics to mitigate contract vulnerabilities, proposing the use of a symbolic execution tool named Oyente [12].

CONCLUSION AND FUTURE WORK

We conducted a Systematic Mapping to investigate which primary development processes have been used in, and which factors have been influencing Blockchain-based IoT building.

Our research aims to provide an overview of the prevailing best practices delineated in the literature for constructing an initial ontology model for Blockchain-based IoT projects. Given the novelty of the Blockchain-based IoT research field, a majority of the literature, including books, technical reports, and other works, has emerged over the past 5 years. We have documented various frameworks, models, methodologies, and other initiatives in Blockchain-based IoT that adhere to established development procedures and strive to establish a foundational knowledge base. Through this exploration, we have identified essential requirements.

Hence, the primary contribution of this study lies in comprehending the domain of Blockchain-based IoT development, with the objective of establishing optimal methodologies for crafting devices (or things) that instil greater trust in their utilization (or transactions). These are the essential requirements for building a Blockchain-based IoT.

REFERENCES

1. Das ML. Privacy and security challenges in internet of things. In Distributed Computing and Internet Technology: 11th International Conference, ICDCIT 2015, Bhubaneswar, India, February 5-8, 2015. Proceedings 11. Springer International Publishing. 2015; 33–48.
2. Ho G, Leung D, Mishra P, Hosseini A, Song D, Wagner D. Smart locks: Lessons for securing commodity internet of things devices. In Proceedings of the 11th ACM on Asia conference on computer and communications security. 2016 May 30; 461–472.

3. Amoozadeh M, Raghuramu A, Chuah CN, Ghosal D, Zhang HM, Rowe J, Levitt K. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Commun Mag. 2015 Jun 10; 53(6): 126–32.
4. Skarmeta AF, Hernandez-Ramos JL, Moreno MV. A decentralized approach for security and privacy challenges in the internet of things. In 2014 IEEE world forum on Internet of Things (WF-IoT). 2014 Mar 6; 67–72.
5. Gross H, Hölbl M, Slamanig D, Spreitzer R. Privacy-aware authentication in the internet of things. In Cryptology and Network Security: 14th International Conference, CANS 2015, Marrakesh, Morocco, December 10–12, 2015, Proceedings 14. Springer International Publishing. 2015; 32–39.
6. Cueva-Sánchez JJ, Coyco-Ordemar AJ, Ugarte W. A blockchain-based technological solution to ensure data transparency of the wood supply chain. In 2020 IEEE ANDESCON. 2020 Oct 13; 1–6.
7. Ukil A, Bandyopadhyay S, Pal A. IoT-privacy: To be private or not to be private. In 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2014 Apr 27; 123–124.
8. Brodkin J. (2008). Gartner: Seven cloud-computing security risks. [online] InfoWorld. Available from: https://www.infoworld.com/article/2652198/gartner-seven-cloud-computing-security-risks.html.
9. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentralized business review. SSRN. 2008 Oct 31.
10. Buchmann J. Introduction to Cryptography. New York: Springer Science & Business Media; 2013 Dec 1.
11. De Montjoye YA, Shmueli E, Wang SS, Pentland AS. Openpds: Protecting the privacy of metadata through safe answers. PloS one. 2014 Jul 9; 9(7): e98790.
12. Josang A, Haller J. Dirichlet reputation systems. In the IEEE 2nd International Conference on Availability, Reliability and Security (ARES'07). 2007 Apr 10; 112–119.

