Cloud Computing Security in the Aspect of Block Chain

Thade Lakshmi Devi[1], Dr. S. Krishna Mohan Rao[2]
[1]*Research Scholar, Mewar University*
[2]*Research Supervisor, Mewar University*

Abstract **- The Internet was originally built based on trust. After several leaks of information, new risks and challenges are introduced. In recent years, we have used even more new devices based on the Internet. Among the main concerns reported on the literature, we need some special attention to trust, protection of data and privacy. In this scenario, a new paradigm has emerged, some information security based on transparency instead of current models of information security on closed and obscure approaches. Some initiatives have been emerging with Blockchain methods and technologies. In this paper, we propose to build an initial view of the model, as a result of our preliminary investigations, described in the Methodology as systematic mapping. The initial results allowed the perception of the initial requirements involved and open problems. We report on some frameworks, models, approaches, and other Blockchain-based Internet of Things (IoT) initiatives. We also evaluate the adherence of each paper to ten IoT key requirements. This work contributes to the new and still developing body of knowledge in the areas of security, privacy and trust. Our findings are useful not only for future studies in the Academy but also for companies from various sectors present in the Internet ecosystem. They can benefit from the consolidated knowledge and use it to guide the definition of their development processes geared to the new paradigms of the IoT.**

Index Terms **- Block chain; Internet of Things; IoT; Ontology; Privacy; Security.**

INTRODUCTION

Internet of Things (IoT) consists of devices that generate, process, and exchange vast amounts of security and safety-critical data as well as privacy-sensitive information, and hence are appealing targets of various cyber-attacks [1]. Many new networkable devices, which constitute the IoT, are low energy and lightweight. These devices must devote most of their available energy and computation to executing core application functionality, making the task of affordably supporting security and privacy quite challenging. Traditional security methods tend to be expensive for IoT in terms of energy consumption and processing overhead. Moreover, many of the state-of-the-art security frameworks are highly centralized and are thus not necessarily well-suited for IoT due to the difficulty of scale, many-to-one nature of the traffic, and single point of failure [2]. To protect user privacy, existing methods often either reveal noisy data or incomplete data, which may potentially hinder some IoT applications from offering personalised services [3]. Consequently, IoT demands a lightweight, scalable, and distributed security and privacy safeguard. The Blockchain (BC) technology that underpins Bitcoin the first cryptocurrency system [4], has the potential to overcome aforementioned challenges as a result of its distributed, secure, and private nature. The Internet of Things (IoT) is an application domain that integrates different technological and social fields. Despite the diversity of research on IoT, its definition remains fuzzy [1]. With the increase in demand and production of the new devices based on the IoT paradigms, trust and privacy can be even harder for the engineering field. Security flaws in the IoT might lead, for instance, to malicious attacks on secrecy and authentication, silent attacks on service integrity, or attacks on network availability, such as the Denial of Service (DoS). However, privacy and anonymity, on the other hand, are no less severe issues and must be integrated into the design to give users control over their privacy.

In this respect, a new approach has arisen in the security and transparency of information, which takes the place of current models of information security and is based on closed and obscure approaches. Some initiatives have come up with Blockchain methods and technologies [2].

Among the problems of building devices (or embedded systems) based on the IoT paradigm, we can highlight the absence of formalism, language or modeling architecture that enables the unified development and integration among the various
Disciplines of the Semantic Web Stack. We are faced with certain difficulties; in addition to complexity and scalability, there are also time latency problems (currently 10 minutes in the Bitcoin network) and the number of confirmations that must be required for transactions, contradicting IoT conceptions regarding real-time processing [1]. The transactions in the Bitcoin network are visible to all nodes. That presents some difficulties (i.e., transactions carried out only for a few nodes of the network), when we need devices for controlled environments [3].

In this context, it is fundamental to comprehend how the traditional software development could be adapted or evolved to support those new Blockchain-based IoT requirements. What consolidated knowledge is, which factors influence on device development are.

To achieve the goal of this study, we are conducting a systematic mapping of critical factors in IoT paradigms-based, embedded systems building. In this research, we are looking for answers to the following questions: i) has Blockchain-based IoT been constructed to stand on development processes? Also, ii) which Blockchain-based IoTs characteristics, principles or requirements have been considered in Blockchain-based IoT development processes? These research questions will be answered in Section IV.

The main objective of this research is to understand Blockchain-based IoT domains as well as best practices in the field, and to present the latest research about the construction of devices (or things). In addition, this effort contributes to the very new and still growing knowledge regarding security, privacy and trust (areas still very undeveloped) of the IoT. This study is useful not only for future studies in academia but also for companies from various sectors operating in the Internet ecosystem. These companies can benefit from the consolidated knowledge and use it to guide the definition of their development processes geared to the new paradigms of the IoT.

B.The Blockchain overview

The Blockchain is a universal digital ledger that works at the core of decentralized financial systems, such as Bitcoin and many other decentralized systems. The blockchain keeps a record of all transaction made by each participant. Cryptography is used to verify operations and keep information on the blockchain private. Several participants verify each transaction, providing highly redundant verification and are rewarded for the computational work required.

The Blockchain technology has the ability to make the organizations that use it transparent, democratic, decentralized, secure, and efficient. The Blockchain can be used to access to financial services, it presents the primary advantages of the traditional correspondent banking system: i) consistent process standards; ii) more long-range global reconnaissance.

C.The Blockchain Ontology

A first effort to standardize this technology is the BLONDIE (Blockchain Ontology with Dynamic Extensibility) ontology. This OWL ontology can be used to express in RDF different fields of the structures of Ethereum or Bitcoin. It can also be extended to cover other Blockchain technologies. In addition, BLONDIE being OWL has the ability to make explicit knowledge available [3].

Ugarte [3] says that an ideal scenario would be that everyone would use only the original Bitcoin technology, or forks with minimum modifications. The protocol itself is already standardized and well-defined, but since Bitcoin presents many limitations and was not designed for other functionalities besides financial transactions, it is not a realistic scenario Currently, the interoperability between Blockchain technologies is one of the most discussed issues in the Blockchain world and this is where we must focus our efforts on. The devices would be able to communicate to each other directly to update software, manage bugs, and monitor energy usage

RESEARCH METHODOLOGY

The research methodology was divided into four steps. In this paper, we will present only Step #2 (Systematic Mapping) of this Doctoral research, as shown in Fig. 1, and described in detail as follows.

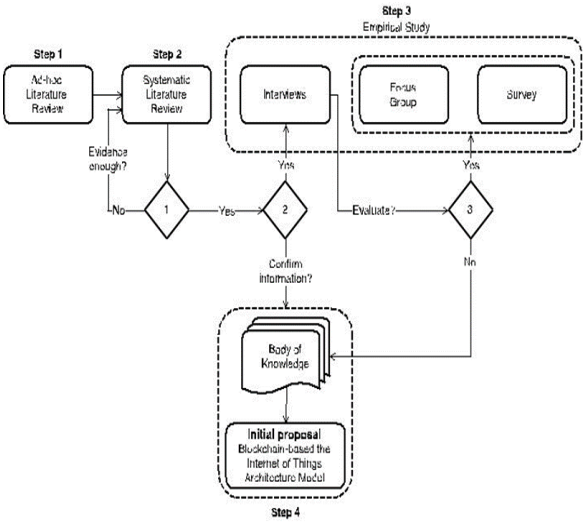

Figure 1. Scientific methodology steps. Adapted from [7]

Security Issues and Risks in Cloud Computing

Gartner in 2008 recognized seven security issues [15] that need to be tended to before organizations switch completely to the cloud computing model.

- Data location: While storing data in cloud some clients might not know where their data is actually located.
- Regulatory compliance: Customers can choose between providers that permit to be examined by third party organizations that check levels of security provided by cloud service providers.
- Data segregation: Since the data in encrypted form from different organizations may be stored in the same place, so a system is required that separates data from different organizations and it should be provided by the cloud service provider.
- Long-term viability: It alludes to the capability to withdraw an agreement and all information if the current supplier is bought out by another firm.

CURRENT TRENDS AND CHALLENGES

The main trends and challenges discussed by the authors of the included papers about Blockchain-based IoT are described in this section.

One author [4] says that security flaws in the IoT may lead, for instance, to malicious attacks on secrecy and authentication, silent attacks on service integrity, or attacks on network availability such as the DoS. Privacy and anonymity, on the other hand, are no less serious issues. IoT devices are natural “collectors and distributors of information”, so they represent a unique challenge to individual privacy.

In particular, the challenges include the ubiquitous interaction of users with smart objects and groups of things, as well as the uncontrolled concentration of such data on platforms lacking in transparency, perhaps systematically exposing users to several threats, such as identification, localization, monitoring, tracking, surveillance, manipulation, profiling, targeted advertising, data linkage, and even social engineering.

The authors in [16] investigated which are the main factors affecting the levels of integrity, anonymity, and adaptability of the blockchain. They should further analyze what are the security properties provided by the Proof of Work, which up to now is one of the key factors allowing for the achievement of distributed consensus.

The Ethereum platform supports a feature to encode rules or scripts for processing transactions through smart contracts. The authors in [10] investigated the security of running smart contracts based on Ethereum in an open distributed network. According to the authors [10][11] there are several new security problems. These bugs suggest subtle gaps in the understanding of the distributed semantics of the underlying platform. Those authors propose ways to enhance the operational semantics to make contracts less vulnerable through a symbolic execution tool called Oyente.

Blockchain has recently attracted the interest of stakeholders from the most varied sectors, from finance and healthcare to utilities, real estate, and the government sector. That explosion Risks in Cloud Computing

The six specific areas of cloud computing where substantial security attention is required are as follows:

- Security of data in transit.
- Security of data at rest.
- Cloud legal and regulatory issues.
- Robust separation between data belonging to different customers.
- Authentication of users/ applications/ processes.
- Incident response.

Threats in cloud computing

Threats in Cloud computing confronts the same amount of security threats that are at present found in the current computing platforms, networks, intranets, internets in enterprises. These dangers, risk vulnerabilities come in different structures.

The Cloud Security Alliance (Cloud Computing Alliance, 2010) did a research on the threats facing cloud computing and it recognized the flowing major threats:

- Failures in Provider Security
- Attacks by Other Customers
- Availability and Reliability Issues
- Legal and Regulatory Issues
- Perimeter Security Model Broken
- Integrating Provider and Customer Security Systems
- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces

CONCLUDING REMARKS 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. The ultimate goal of our research is to present the current panorama about best practices outlined in the literature to develop an initial Blockchain-based ontology model for IoT projects. The Blockchain-based IoT research area is so new and most of the papers and publications (such as a book, a technical report and others works) are concentrated in the last five years We reported on some frameworks, models, approaches, and other Blockchain-based IoT initiatives that present adherence to well-known development processes and endeavor to build an initial body of knowledge. We detected key requirements on the.

Thus, the main contribution of this paper is the under-standing of the realm of Blockchain-based IoT development, and we aim to establish best practices in the construction of devices (or things) that inspire more confidence in their use (or transactions). These are the essential requirements for building a Blockchain-based IoT, and we have identified.

REFERENCE

[1] Das, ManikLal, "Privacy and Security Challenges in Internet of Things," Distributed Computing and Internet Technology, pp. 33-48, 2015.

[2] Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D. and 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.

[3] M. Amoozadeh et al., "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," IEEE Communications Magazine, vol. 53, no. 6, pp. 126-132, 2015.

[4] Skarmeta, Antonio F., Jose L. Hernandez-Ramos, and M. Moreno., "A decentralized approach for security and privacy challenges in the internet of things," in nternet of Things (WF-IoT), 2014 IEEE World Forum on, 2014.

[5] H. Gross; M. Holbl, D. Slamanig, and R. Spreitzer, "Privacy-Aware Authentication in the Internet of Things," Cryptology and Network Security. Springer International Publishing, pp. 32-39, 2015.

[6] A. Ukil, S. Bandyopadhyay and A. Pal, "IoT-Privacy: To be private or not to be private," in Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on., Toronto, 2014.

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[8] Decker, Christian, Jochen Seidel, and Roger Wattenhofer., "Bitcoin Meets Strong Consistency.".

[9] J. Buchmann, "Introduction to cryptography.," Springer Science & Business Media, 2013.

[10] T. Project. [Online]. Available: https://www. torproject.org/.

[11] de Montjoye, Yves-Alexandre, et al., "openpds: Protecting the privacy of metadata through safe answers," PloS one 9.7 (2014).

[12] Jøsang, Audun, and Jochen Haller., "Dirichlet reputation systems," in Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on., 2007.