

|  |  |
| --- | --- |
| IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 16, NO. 11, NOVEMBER 2020 | 7081 |
|  |  |

Designing Secure Lightweight

Blockchain-Enabled RFID-Based

Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment

Srinivas Jangirala*, Member, IEEE*, Ashok Kumar Das*, Senior Member, IEEE*,



and Athanasios V. Vasilakos*, Senior Member, IEEE*

***Abstract*—Secure real-time data about goods in transitin supply chains needs bandwidth having capacity that is not fulfilled with the current infrastructure. Hence, 5G-enabled Internet of Things (IoT) in mobile edge comput-ing is intended to substantially increase this capacity. To deal with this issue, in this article, we design a new effi-cient lightweight blockchain-enabled radio frequency iden-tification (RFID)-based authentication protocol for supply chains in 5G mobile edge computing environment, called lightweight blockchain-enabled RFID-based authentication protocol (LBRAPS). LBRAPS is based on bitwise exclusive-or (XOR), one-way cryptographic hash and bitwise rotation operations only. LBRAPS is shown to be secure against various attacks. Moreover, the simulation-based formal se-curity verification using the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool assures that LBRAPS is secure. Finally, it is shown that LBRAPS has better trade-off among its security and functionality features, communication and computation costs as compared to those for existing protocols.**

***Index Terms*—Authentication, blockchain, 5G mobileedge computing, radio frequency identification (RFID), security, supplychain.**

1. INTRODUCTION

G IS a combination of various technologies as well as

**5**mechanisms that is expected to land into the future networks

Manuscript received July 21, 2019; revised August 29, 2019; accepted September 16, 2019. Date of publication September 19, 2019; date of current version July 29, 2020. This work was supported by the Ripple Centre of Excellence Scheme, Centre of Excellence (CoE) in Blockchain (Sanction no. International Institute of Information Technology (IIIT)/R&D Office/Internal Projects/001/2019), IIIT Hyderabad, India. The Associate Editor coordinating the review of this manuscript and approving it for publication was Dr. K.Y. Chan. Paper no. TII-19-3242 *(Corresponding* *author: Ashok Kumar Das.)*

S. Jangirala is with Jindal Global Business School, O. P. Jindal Global University, Haryana 131 001, India (e-mail: [sjangirala@jgu.edu.in)](mailto:sjangirala@jgu.edu.in).

A. K. Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India (e-mail: [iitkgp.akdas@gmail.com)](mailto:iitkgp.akdas@gmail.com).

A. V. Vasilakos is with the Department of Computer Science, Electrical and Space Engineering, Lulea˚ University of Technology, 971 87 Lulea,˚ Sweden and Computer Science and Technology, Fuzhou University 350 108, Fujian, China (e-mail: [th.vasilakos@gmail.com)](mailto:th.vasilakos@gmail.com).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2019.2942389

in order to fulfill maximum capacity and performance demands. It is expected that the design of 5G networks would spin around virtualization along with programmability of various networking services [1]. It is visualized that transition to 5G will be smoothed by today’s emerging technologies, such as blockchain, software defined networking (SDN), network functions virtualization, Internet of Things (IoT), mobile edge computing (MEC), and fog computing. In addition, SDN and network function virtualization (NFV) support new tools that will strengthen pliability in designing networks [2].

MEC plays as a key enabler for IoT and also for mission-critical, vertical solutions. It is considered as one of the primary architectural conceptualizations and technologies [3]. Recently, Rahman *et al.* [4] presented an in-home therapy management so-lution. It enables the IoT smart devices as well blockchain-based decentralized MEC paradigm to assist low-latency, anonymous, secure, and always-accessible spatio-temporal multimedia ther-apeutic data communication within an on-demand data-sharing layout for healthcare applications. 5G technology implemen-tation is treated as another instance to possibly take advantage from the blockchain to smooth-running processes. The combina-tion of 5G and blockchain technology will have much potential to unbind a surge of economic value. In addition, the power of 5G coverage through its reduced latency, high speeds and capacity will permit the IoT devices to become widely used [5]. The “Communications Service Providers (CSPs)” require to grasp heterogeneous kind of access nodes and also multiple access approaches for the 5G promising of ubiquitous access across multiple networking environments [6]. Thus, it will remain a central challenge in the future to pick the fastest access node for each node (machine). Hence, the blockchain technology shown in Fig. 1 enables a new generation of access technology selection mechanisms that are essential for 5G networks [6].

Application of the blockchain technology with 5G can save companies millions of dollars in terms in operating costs. In addition, this will also help in avoiding its potential legal fees appearing from disputes. Consider a smart contract pro-totype in a typical supply-chain process that can streamline the supply-chain process and also permit the automatic payment of goods upon receipt. It will help in eliminating the necessity

1551-3203 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.

See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: University of New South Wales. Downloaded on November 20,2020 at 02:19:00 UTC from IEEE Xplore. Restrictions apply.

7082 IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 16, NO. 11, NOVEMBER 2020

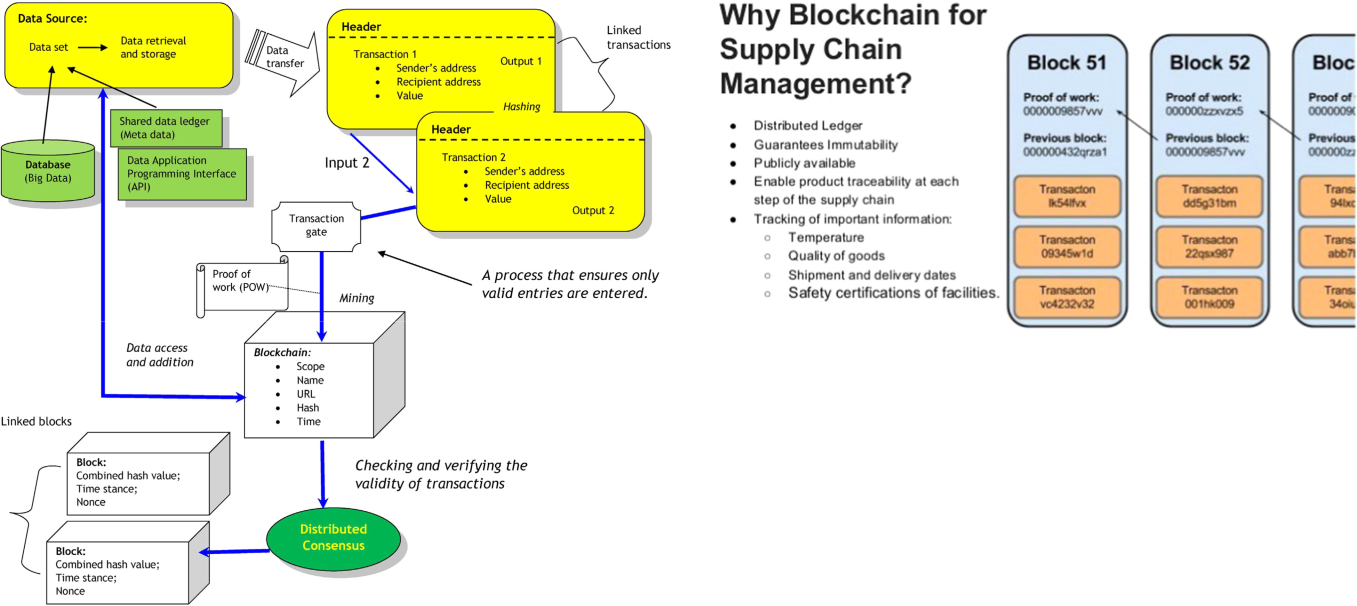


Fig. 1. Basic architecture of blockchain technology [7].

of having to deal with accounts receivables and paying for billing department personnel to track down distributors with outstanding invoices [1]. Therefore, the use of blockchain technology with 5G helps in tracking a shipment so that both the manufacturer and the distributor can immediately know exactly where they stand with respect to a volume incentive rebate. The information is instantly loaded onto the blockchain. This helps both the manufacturer and distributor to see in real time how many units of a particular model have been sold in a territory for determining whether the conditions precedent to earn a volume incentive rebate have been met or not. Therefore, if the information uploaded onto the blockchain shows that the distributor satisfies all the conditions precedent, the rebate would be issued automatically to the distributor, without the need for the distributor to follow up with the manufacturer for payment.

The blockchain users can either generate randomly or pre-define the block content. A set of transactions (data block) is cryptographically protected by the use of a “collision-resistant cryptographic one-way hash function,” such as Secure Hash Algorithm (SHA 256) for assuring anonymity, compactness as well immutability of the block. In addition, the ledger along with its contents are reproduced and synchronized in a “Peer-to-Peer (P2P)” network across several peers, which will create a distributed ledger. Even if the blockchain is a part of “Distributed Ledger Technologies (DLT),” a chain of blocks is not also utilized by all DLTs [8]. Such a technology is referred to as the blockchain. There are three types of blockchain; 1) per-missioned blockchains, 2) permissionless (public) blockchains, and 3) consortium blockchains [9].

The “distributed consensus” protocol assures that a majority of blockchain network peers agree on the precise condition of the shared ledger. Some of the used distributed consensus algorithms work without a central manager in the network, where the blockchain nodes accomplish the verification of a transaction in different manners of consensus, such as PoW

Fig. 2. Blockchain–supplychain management [13].

Proof of Work (Pow), Proof of Stake (Pos), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), and Raft [9]–[11]. The major utilization of blockchain is included in the Bitcoin and cryptocurrency, where the PoW is utilized as a consensus protocol and the computing power as a system in order to determine the selected peer [9].

There are multiple blocks in a blockchain ledger where each block contains two parts. The first part contains the transactions or facts which need to be stored at the database, and such kinds of transactions may be “monetary transactions,” “supplychain data,” “health data,” “system logs,” and “traffic information.” On the other hand, the second part contains the header that consists of information about its block (e.g., timestamp, hash values of its transaction and the previous block). Hence, the set of the existing blocks constitutes a chain of linked and ordered blocks. If the chain length becomes longer, it will be a much difficult task for an adversary (a malicious user) to falsify it. In order to modify or swap a transaction on a block the adversary requires to do the following two tasks: 1) it is essential to modify all the subsequent blocks as the blocks are linked with their hashing, and 2) it is also essential to update the version of the block chain that each participating node stores it. In Fig. 2, we have shown an example for a popularized blockchain–supplychain management. It is worth noticing that the blockchain ledgers create a shared and secure record of “supplychain information flows” [12].

With the extensive vendor network and supply chain exper-tise, it can be possible to lower the costs and also to streamline the operations while focusing on various strategic goals, such as “white glove in-store/in-home delivery, assembly and debris removal, limited access/final mile delivery, store display/fixture rollouts, pool distribution, charge-back avoidance strategies, drop-trailer programs, warehousing/cross-docking, and reverse logistics” [13].

In the following section, we briefly describe the mobile edge computing (MEC)-enabled artificial intelligence (AI) and IoT with blockchain.

1. MOBILE EDGE COMPUTING-ENABLED AI AND IOT WITH BLOCKCHAIN

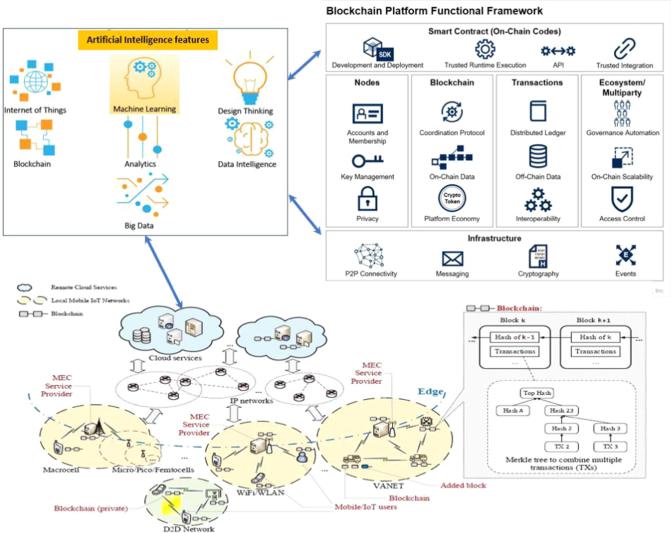
MEC is a new network epitome that applies cloud computing

1. capabilities inside the portable access system of mobile units (MUs). It also provides information technology services

Authorized licensed use limited to: University of New South Wales. Downloaded on November 20,2020 at 02:19:00 UTC from IEEE Xplore. Restrictions apply.

|  |  |
| --- | --- |
| JANGIRALA *et al.*: DESIGNING SECURE LIGHTWEIGHT BLOCKCHAIN-ENABLED RFID-BASED AUTHENTICATION | 7083 |
|  |  |

Fig. 3. MEC-enabled AI and IoT with blockchain (Adapted from [14], [15]).



to turn into an innovation technology. MEC can successfully provide a new ecosystem with a value chain that can utilize it to relocate serious computing tasks with in the range of MUs as pointed out by the “European Telecommunications Standards Institute (ETSI)” to standardize MEC [16]. The design needs to deploy MEC architectures on constrained mobile edge devices is as follows. MEC should effectively minimize the effects of network equipment and also effectively support the innovation advantages of a unique mobile experience. As shown in Fig. 3, the radio access network consists of MECs, which are located very close to the MUs such that with low latency and higher bandwidth, the Quality of Service (QoS) and Quality of Experi-ence (QoE) can be achieved. In addition, MEC plays a key role in developing the technology such as 5G [17] so that the established standards like scalability, delay, and programmability can be met [18].

IoT is a typical application of Blockchain technologies that utilizes the advantages of blockchain [19], [20]. The smart devices in the IoT systems are generally connected to various physical objects, such as actuators, sensors, and mobile devices which can sense, communicate, and exchange the information in real-time over the Internet. These IoT devices are better utilized in smart transport, healthcare, logistics, and manufactur-ing [21]–[24]. It is very clear that IoT devices help the system to communicate with the real-time data. The IoT devices are in gen-eral very low-powered, and they are deployed geographically depending upon the application and sometimes possibly mobile. Thus, the utilization of low computational and limited energy resources of IoT devices when integrated with blockchain helps the IoT systems better in mining the process well and producing the real-time data efficiently and securely. The major challenge to any system and environment is to deploy blockchain in other low computational devices. According to [14], as shown in Fig. 3, MEC can be very much handy in enriching the supply of the resources by embedding the blockchain computing as

and when some demands arise. By enriching local computation power, blockchain deployment by enabling edge computing in IoT frameworks helps understanding PoW befuddles, hash-ing, encryption algorithms, and potentially consensus. Very recently, IBM provided the Watson IoT platform that utilized a private blockchain ledger to manage the IoT data, which enhances the IBM’s business-level by integrating their cloud services [25].

Recently, radio frequency identification (RFID) has gained popularity in various applications, such as “logistics,” “material flow systems” as well as “supply chain management” as a representative technology for automatic identification and also for data capture. Integrating promising technologies such as RFID can assist improving the effectiveness of information flow in supply chain. The partners in the supply chain may access information and practice quality control based on the data shared through RFID and other technologies [26].

Another perceptible field is AI which is expanding with huge balance by empowering a machine to learn, actuate, and alter subject to data it assembles with the cognitive functions. According to the recent market research, the predictions say that the market of AI will raise up to 13 trillion US dollars constantly by the year 2030. In the emerging concept, the decentralized AI has got much attention where it is basically a blend of AI and blockchain [27]. The decentralized AI engages to process and perform analytics or decision making on trusted, deliberately stamped, and secure shared data that has been executed and secured on the blockchain, in a scattered and decentralized style, without the trusted third parties or center individuals [27],

1. AI is known to work with gigantic volumes of data, and blockchain has now been anticipated as a trusted in stage to store such data [29].

Basically, the AI algorithms help to come-up with the final decisions which actually rely on the data or the information learning from the inferred data. When the data is collected from entrusted platform which is considered to be reliable, secure, and trusted, it gives a better result while executing the machine learning algorithms. It is believed that blockchain can assist as a distributed ledger on which information can be put away and ex-ecuted in a manner that is cryptographically marked, approved, and concurred on by all mining nodes. Blockchain information can be then put away with high integrity and strength, and it cannot be tampered [30]. To make decisions on ensuring the smart contracts the use of machine learning algorithms are very handy and also for measuring the performance well. Due to the efficiency in decision making the outcome of the machine learning algorithms can be trusted and undisputed.

The blend of AI and blockchain in 5G-enabled MEC can make secure, perpetual, and decentralized framework for the exceedingly unstable information that the computer-based in-sight driven systems should be able to assemble, store, and utilize [31]. This idea brings a noteworthy enhancement to verify the data in different fields, including medicinal, personal, banking and budgetary, exchanging, and lawful information. As a result, this article focuses on secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G MEC environment that can use the AI methods deployed

Authorized licensed use limited to: University of New South Wales. Downloaded on November 20,2020 at 02:19:00 UTC from IEEE Xplore. Restrictions apply.

7084 IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 16, NO. 11, NOVEMBER 2020

for better predictions, analysis, and provision of data authen-ticity and trustworthiness via blockchain in the realm of 5G MEC.

In the following, we provide some key characteristics that are shared by the commercial transactions which use the blockchain technology.

* 1. *Real-time Records:* Distributed ledgers are refreshed unin-terruptedly as transactions and different occasions may happen with programming or computerizing the procedure. In addition, the computerized procedure and absence of an incorporated record guardian can increase efficiencies and also produce cost savings [32].
  2. *Immutable Records:* Blockchain innovation empowers sub-stances to create permanent and changeless transaction records. This capacity offers a conspicuous business advantage, but it can likewise raise administrative hazard for some parties [32].
  3. *Anonymity:* Blockchain innovation creates it less demand-ing for the network users to be pseudonymous, which has repercussions for administrators of networks subject to various aspects, such as antimoney laundering (AML) and know-your-customer (KYC) regulations.
  4. *Cybersecurity Risk:* For an assortment of reasons,blockchain systems have turned out to be the most loved focus for hackers. The security incidents have ranged from ordi-nary administration disturbances to growing genuine burglaries of sensitive information as well as valuable cryptocurrencies even if the decentralized blockchain structured networks make them stronger against various network-wide attacks including tampering of data.
  5. *Tax Implications:* Blockchain transactions including virtualcurrency can provide ascent to unforeseen tax consequences relying upon how the appropriate tax authority treats “virtual currency.” For instance, the US Internal Revenue Service regards “virtual currency” as property in the sense that a transaction may create the requirement in order to recognize a gain or loss on the exchanged cryptocurrency.

1. *Motivation*

RFID has several industrial applications today, such as man-agement in supply chain and airline baggage, and automated payment systems. A potential blockchain-based solution to address these can be spearheaded through integration with IoT devices as shown in Fig. 4. We can consider the RFID tags on shipment containers being scanned at each node of a supply chain, and sending that information to the blockchain network [33]. The information can then be timestamped and permanently logged on a blockchain ledger. The immutable and transparent nature of these ledgers can allow each party in a given supply chain to access shipment information in a trustworthy and reliable fashion. Blockchain technology is promising is many regards, but its application in supply chains can potentially prove to be the most fruitful.

The sensitive RFID data is transmitted over the public Internet and also stored in various devices. Therefore, it is essential to have communication security protocols which make RFID systems secure because RFID-enabled devices deal with various

Fig. 4. RFID in supplychain from manufacturer to retailer [34].



sensitive objects (e.g., passports and identity documents). Also, it is needed that the confidential RFID data should not be leaked in case of the real-time applications or health care monitoring system.

Several common authentication security protocols have been suggested in the literature. The existing protocols need a database to be stored in the server side to help the authenti-cation process. Apart from the multiorganization participation, we now consider another circumstance as the supply chain. Assume there are various departments or branches in a single organization, and specifically, some of them are geologically deployed or these are even appropriated in various nations. How-ever, various tasks and management related to an organization need departments to allocate some information of the tags. In addition, a prerequisite that new RFID framework as well as protocols should satisfy for an organization’s practical require-ments is to assure the privacy of the departments. Moreover, the synchronization is also an unwieldy issue in distributed RFID frameworks when a new tag is incorporated or in each round the authentication message is refreshed. Consequently, in this article we design a new “blockchain-based mutual authentication RFID protocol” that can fulfill the above needs.

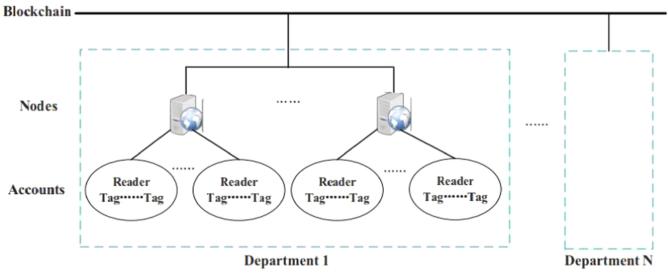
We set forward the necessities that the distributed RFID framework requirements are not yet accessible in the exist-ing protocols. A multidepartment collaboration situation is considered to exhibit a “blockchain-based distributed RFID framework” model and then to depict the proposed authentica-tion protocol. Through the proposed blockchain-based scheme, the following objectives are accomplished at the same time:

1. security against several attacks; 2) traceable and unchange-able communication documentations; 3) each department needs its own secret tag information that is not incorporated in servers; and 4) interdepartment distribution of inconsiderable tag data for authentication purpose without involving a central server or “trusted third parties.”

Authorized licensed use limited to: University of New South Wales. Downloaded on November 20,2020 at 02:19:00 UTC from IEEE Xplore. Restrictions apply.

|  |  |
| --- | --- |
| JANGIRALA *et al.*: DESIGNING SECURE LIGHTWEIGHT BLOCKCHAIN-ENABLED RFID-BASED AUTHENTICATION | 7085 |
|  |  |

Fig. 5. Multidepartment cooperation distributed RFID architecture [35].



*B. System Models*

The requirements of RFID system within a company can be met in a “private blockchain with *Raft* consensus mechanism.” Here, we consider the “multidepartment cooperation distributed RFID” system that is illustrated in Fig. 5. Multiple departments keep a private blockchain together and also execute the same authentication procedure [35]. This system model can ensure the sharing of insensitive tag information for authentication while protecting the secret tag information within department itself through the following settings [35].

* 1. Various servers run in each department, which are known as the nodes on blockchain. Each node has a set of ac-counts that are linked with the tags and readers, and these are retrieved by all nodes containing in the blockchain.
  2. The blockchain can generate a 20-byte public key ad-dress, known as an account identifier (in Ethereum), when the tag or reader ID as password is provided as input. Each department is associated with the “real object-ID-account address” mapping table that is kept in secret place from the entire system.

1. *Authentication Model:* As shown inFig. 5, we assume thatthere are *N* departments in the blockchain. Each department is privileged with nodes (Supplychain) and accounts (Reader-Tag). Here, the reader *R* initiates the process with a certain key for tag verification to prove its identity. The tag *T* proceeds further computations with the current timestamp and balance in the blockchain, and gives a challenge to the reader *R*. If the challenge is solved successfully, the reader computes and processes the authentication message to the supply chain. The supplychain gets the message from the reader and validates the received message. Once it is proven to be successful, the supplychain acknowledges the supply amount and goes on to establish the session key which can be shared with the tag for future communications. This entire process happens via the reader *R*, and both the supplychain node and the tag *T* establish a session key and update the blockchain balance successfully.
2. *Threat Model:* Similar to any other networks, we applythe widely-accepted “Dolev-Yao (DY) threat model in which an adversary can not only can eavesdrop the communicated messages among the various entities but can also modify, delete, or insert fake messages in between the communication” [36] including to perform several potential attacks such as “im-personation, replay, man-in-the-middle, and ephemeral secret leakage (ESL) attacks.” The “Canetti and Krawczyk’s adversary

model (CK-adversary model)” [37] is a current *de facto* stronger model as compared to the DY model, which is also applied in many recent authentication protocols. The CK-adversary model allows “the adversary apart from his/her the abilities as performed using the DY model, he/she can also compromise the session states along with secret information including secret keys.” Thus, even if the session states along with secret informa-tion are compromised in a particular session, these compromised information must not lead to compromise the secrecy of other parties’ credentials. Hence, it is also important that under the CK-adversary model the forward and backward secrecy need to be preserved in an authentication protocol.

*C. Research Contributions*

We list the main research contributions as follows.

* 1. A new lightweight blockchain-enabled RFID-based au-thentication protocol, called lightweight blockchain-enabled RFID-based authentication protocol (LBRAPS), has been proposed, which is based on bitwise exclusive-or (XOR), one-way cryptographic hash, and bitwise rota-tion operations. LBRAPS contains two phases, namely initialization and authentication and key agreement.
  2. LBRAPS is examined for its security part against various attacks against an active (passive) adversary.
  3. The simulation-based formal security verification using the broadly-accepted “Automated Validation of Internet Security Protocols and Applications (AVISPA)” tool assures that LBRAPS is also secure.
  4. LBRAPS has better tradeoff among its security and functionality features, communication, and computation costs as compared to those for other related existing protocols.

1. *Article Outline*

The rest of this article is organized as follows. The related work is discussed in Section III. The proposed blockchain-based authentication protocol (LBRAPS) is discussed in detail in Section IV. The evaluation of LBRAPS for its both secu-rity is done in Section V. The formal security verification using AVISPA-based software simulation tool is provided in Section VI. In Section VII, we present the efficiency of LBRAPS in terms of security and functionality features, computation, and communication costs. Finally, Section VIII concludes this article.

1. RELATED WORK

The blockchain technology has several benefits for the sup-ply chain application. However, there are many barriers to its widespread adoption. The security and privacy concerns related to the integration of RFID technology in blockchain is considered as one of the important barriers.

He *et al.* [38] designed an elliptic curve cryptography (ECC)-based RFID authentication protocol that integrates with an ID verifier transfer mechanism. After that, Lee and Chien [39] demonstrated that He *et al.*’s protocol was vulnerable to active

Authorized licensed use limited to: University of New South Wales. Downloaded on November 20,2020 at 02:19:00 UTC from IEEE Xplore. Restrictions apply.

7086 IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 16, NO. 11, NOVEMBER 2020

tracking attack. To withstand such an attack, they also designed an improved RFID authentication protocol.

Liao and Hsiao [40] designed another ECC-based RFID authentication protocol that was integrated with ID-verifier transfer mechanism. However, later Li *et al.* [41] found that the scheme of Liao and Hsiao [40] was not resilient against forward security and ID-verifier confidentiality. To resolve these vulnerabilities, they further proposed an efficient authentication approach.

He and Zeadally [42] provided a detailed review on various ECC-based RFID authentication mechanisms. They found that only some of the security attributes are satisfied by the analyzed RFID-based authentication protocols. Various authors also designed several heavy-weight authentication protocols [20], [43]–[46].

Fan *et al.* [47] designed two RFID mutual authentication schemes with cache in the reader for IoT environment that is also suited in 5G. Their first scheme is called “lightweight radio frequency identification mutual authentication protocol with cache in the reader (LRMAPC),” whereas the second scheme is called “ultralightweight RFID mutual authentication protocol with cache in the reader (ULRMAPC).” However, Li *et al.* [48] analyzed LRMAPC and demonstrated that it fails to achieve reader impersonation, tag forgery, and message eavesdropping attacks. Though both LRMAPC and ULRMAPC are lightweight and ultralightweight protocols, respectively, they do not provide untraceability property.

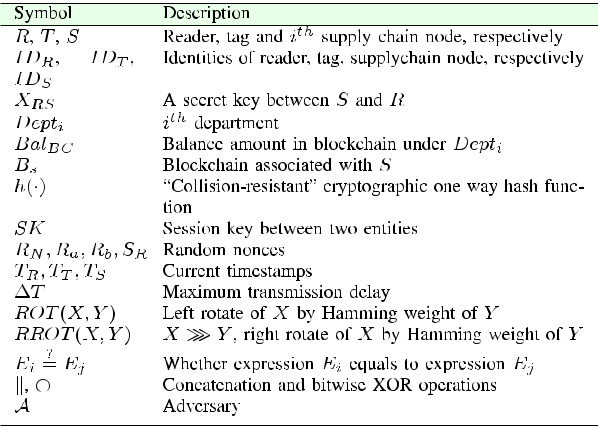
Toyoda *et al.* [49] designed a system for blockchain-based product ownership management problem for RFID attached products for anticounterfeits in order to apply it in the post supply chain. They designed a full-fledged security protocol which can enable each entity, including supply chain partners as well as customers for transferring and proving the “ownership of RFID tag-attached products” that are based on “Electronic Product Code (EPC).” Since the EPC is transmitted as a fixed component during the entire process, an adversary can monitor the movement of the RFID tag-attached products based on the transmitted EPC value.

Mujahid *et al.* [50] proposed an ultralightweight primitive, known as the “pseudo-Kasami code.” In their primitive, the secrecy for RFID systems is achieved by means of utilizing the unpredictable property of secret keys. Besides this, they proposed a mutual authentication RFID protocol based on their pseudo Kasami-code, bitwise XOR, bitwise rotation, and Hamming weight. Another RFID protocol, known as Gen2V2 proposed in [51], adds an extra security feature (called the untraceable command) to the protocol [50]. The “untraceable command” entitles a tag to reveal its secret credentials, such as EPC and user memory to restricted readers only. Since any unauthorized reader assembling with Gen2V2 protocol can demand as a privileged reader itself and can also undo a tag’s untraceable feature, and thus, such security feature (untraceable command) leads to security attacks.

A “low-cost authentication protocol for the distributed database RFID system (hierarchical group-index based lightweight authentication protocol (HGLAP) protocol)” was also proposed in [52]. HGLAP is efficient because it helps in reducing the search time for a tag identity in the back-end

TABLE I

NOTATIONS USED IN LBRAPS



database. The challenge-response based mutual authentication protocol (CRMAP) protocol designed in [53] is a kind of “challenge-response authentication protocol,” which relies on a “cryptographic collision-resistant hash function.” CRMAP was shown to be robust against spoofing as well as replay attacks. Though there are some protocols proposed for distributed RFID systems [52], [53] in the literature, these protocols hinge on either a “distributed database” or a “central trusted server.”

Sidorov *et al.* [54] designed an “ultralight-weight RFID protocol for blockchain-enabled supply chains.” However, the main issue related to their design was that an adversary can easily obtain the tactful credentials by means of capturing the communicated messages as it relies on only bitwise rotate operation. Masoumeh and Mahyar [55] also recommended that single or multiple applications of “bitwise rotate (ROT)” with “bitwise XOR” operations do not converge to build a secure protocol. Therefore, to construct a secure protocol without any cryptographic primitives is difficult. As a result, we feel that there is a requirement to construct a “robust and efficient RFID protocol” that can abolish the security flaws that are still found in the previous protocols for the purpose of integrating it with blockchain infrastructure.

IV. THE PROPOSED SCHEME

In this section, we aim to construct a new lightweight blockchain-enabled RFID-based authentication protocol, called LBRAPS. The LBRAPS is categorized into two phases:

1. initialization phase and 2) authentication and key establish-ment phase. Table I shows the notations and their significance, which are used in LBRAPS.

Supply chain management is regarded as one of the important domains where the blockchains are good fits for the following reasons [56]. The life-cycle of a product has a flow in the value chain (for example, from the production to consumption). Thus, the data created in each step needs to be documented as a transaction and hence, a permanent history of the product, which constitutes the blockchain *Bs* associated with the supplychain node in the proposed protocol (LBRAPS). The blockchain technology can effectively contribute to the following [56]: “1) recording every single asset (from product to containers)

Authorized licensed use limited to: University of New South Wales. Downloaded on November 20,2020 at 02:19:00 UTC from IEEE Xplore. Restrictions apply.

|  |  |
| --- | --- |
| JANGIRALA *et al.*: DESIGNING SECURE LIGHTWEIGHT BLOCKCHAIN-ENABLED RFID-BASED AUTHENTICATION | 7087 |
|  |  |

as it flows through the supply chain nodes, 2) tracking orders, receipts, invoices, payments, and any other official document, and 3) tracking digital assets (such as warranties, certifications, copyrights, licenses, serial numbers, and bar codes) in a unified way and in parallel with physical assets.” In addition, the blockchain can also contribute effectively in sharing information about the production process, delivery, maintenance, and wear off of products between the suppliers and vendors through its decentralized nature.

*A. Initialization Phase*

To initialize the protocol, we consider the tag or reader ID as the password, and for each account identifier the blockchain generates public key address. Therefore, the tag stores the tuple *{IDT* *, BalB C* *}*, where the tag ID and balance amount in blockchain under *Depti* are *IDT* and *BalB C* , respectively. Similarly, each reader also stores *{IDR* *}* in its memory, whether the reader ID is *IDR* . Furthermore, the supply chain node (*S*) and the reader (*R*) will share a secret key *XRS* = *h*(*IDS* *Bs*

*IDR* )which is private, where *Bs* represents the blockchainassociated with *S*.

Since the reader (*R*) initiates the transaction and sends the transaction request to the tag (*T* ), the *R*’s account must have balance initially while creating account or mining which is realistic in nature. Therefore, the balance of each tag account in the blockchain is *BalB C* and for any new transactions it is initialized as *Bal*New = *BalB C* +*S*Amount, where *S*Amount is the amount related to the supply chain transaction.

*B. Authentication and Key Agreement Phase*

The phase is executed by the participants; the reader (*R*), the tag (*T* ), and the supply chain node (*S*), which is described by the following steps for mutual authentication purpose and also establishment of session key between *T* and *S*. The illustration of the LBRAPS is also shown in Fig. 6.

*Step 1: R → T* : *MSG*1= *{MR , CR , TR }*

The reader (*R*) generates a random number *RN* and current timestamp *TR* . Further, it computes *MR* = *ROT* (*RN ⊕IDT ⊕TR , TR ⊕ IDT* )and *CR* = *h*(*MR IDT RN* ), and then transmits the requestmessage *MSG*1 = *{MR* *, CR* *, TR* *}* to the tag (*T* ) via open channel.

*Step 2: T → R*: *MSG*2= *{CT , AuthR , MT , TT }*

The tag *T* receives the message *MSG*1 from the reader (*R*) first checks the validity of timestamp

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *T* | *R* | using the criteria | *|* | *T* | *R −* | *R* | *|* | *<* | *R* |  |
|  |  |  | *T ∗* |  | *T* , where *T ∗* |  |
| and | | *T* are receiving time of the message *MSG*1 | | | | | | | |  |

and “maximum allowable transmission delay,” respec-tively. If it fails, the phase is instantly terminated by *T* . Otherwise, *T* extracts the random number *RN* of *R* as *RN* = (*MR* ≫ (*IDT* *⊕* *TR* ))*⊕* *IDT* *⊕* *TR* , and calculates *CR* = *h*(*MR* *IDT* *RN* ) and checks

?

*CR* = *CR* . If it is valid, *T* also computes *CT* = *h*(*RN ⊕IDT ⊕Bal*New), *MT* = *ROT* (*RN ⊕IDS ⊕TT , TT ⊕ IDT* ), and *AuthR* = *h*(*CT RN MT IDT*

*TT* ). After this computations, the tag *T* sends theresponse message *MSG*2 = *{CT* *, AuthR* *, MT* *, TT* *}* to the reader *R* via open channel.

*Step 3: R → S*: *MSG*3= *{MQ , MP , Reader*check*, TR }* The reader *R* receives the message *MSG*2 from the tag (*T* ) and verifies the authenticity of the received message by validating the timestamp *TR* . If it holds,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *R* | ? | *h*(*CT* | *RN MT* |  |
| further checks if *AuthR* = |  |

*IDT TT* ). If it also valid, *R* then generates tworandom nonces *Ra* and *Rb* at time *TR* , and com-

putes *MP* = *Ra* *⊕* *IDS* *⊕* *Rb* , *MQ* = *XRS* *⊕Rb* , and *Reader*check= *h*(*Ra ⊕IDS ⊕Bal*New *⊕*(*Rb TR* )).

After this computations, the reader *R* sends the mes-sage *MSG*3 = *{MQ* *, MP* *, Reader*check*, TR* *}* to the supply chain node *S* belongs to the department *Dept*1 of the blockchain.

*Step 4: S → R*: *MSG*4= *{SP , SQ , SS , TS }*

The supply chain *S* receives the message *MSG*3 from the reader *R* and checks the validity of timestamp *TR* . If it is valid, *S* automatically starts the predefined smart contract on the blockchain to continue the authentication process. The authentication process is initiated first through the supplychain of blockchain by checking if the *IDT* is in *S*’s database. If it is not there, the process is terminated. Otherwise, *S* gets *BalB C* *−*REC and undergoes the following com-putations: *Rb* = *XRS* *⊕MQ* , *Ra* = *MP* *⊕* *IDS* *⊕* *Rb* , *S*check*A* = *h*(*Ra ⊕ IDS ⊕ BalB C −*REC *⊕*(*Rb TR* )), and *S*check*B* = *h*(*Ra ⊕ IDS ⊕* (*BalB C −*REC+ *S*Amount) *⊕*(*Rb TR* )). Once these computationsare performed, the verification check is done by checking the condition (*S*check*A* = *Reader*check) and if it successful, *S* records *BalB C* *−*REC = *BalB C* . Otherwise, if (*S*check*B* = *Reader*check) is valid, *S*

*S*Amount

acknowledges *IDR* *−−−−→* *IDT* , and also records

*BalB C −*REC= *BalB C −*REC+ *S*Amountin the dis-

tributed ledger *LedgerB C* . Furthermore, *S* generates a random number *SR* at current timestamp *TS* to compute *SP* = *ROT* (*TS* *, IDS* *⊕* *XRS* )*⊕* *ROT* (*SR* *,* *XRS* ), *SQ* = *ROT*(*SR , IDS* )*⊕ ROT*(*TS , XRS* ), *SKS T* = *h*(*IDT ⊕ BalB C −*REC *⊕SR ⊕IDS* ), and *SS* = *h*(*SKS T SR BalB C −*REC). Here, *SKS T* isthe session key initiated by the supply chain node *S* so that the tag(*T* )can also establish the samesession key by authenticating the valid messages. The supply chain node *S* then sends the message *MSG*4= *{SP , SQ , SS , TS }* to the reader(*R*)viaopen channel.

*Step 5: R → T* : *MSG*5= *{SS , RQ , TS }*

The reader (*R*) receives the message *MSG*4 from the supplychain node (*S*) and checks the validity of the received timestamp *TS* . If it does not fail, *R* extracts the random number *SR* of the reader as *SR* = *RROT* (*SQ ⊕ROT* (*TS , XRS* )*, IDS* )and validatesit to authenticate the supply chain node *S* by checking

?

if *SP* = *ROT* (*TS* *, IDS* *⊕* *XRS* )*⊕* *ROT* (*SR* *, XRS* ).

Authorized licensed use limited to: University of New South Wales. Downloaded on November 20,2020 at 02:19:00 UTC from IEEE Xplore. Restrictions apply.

7088 IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 16, NO. 11, NOVEMBER 2020

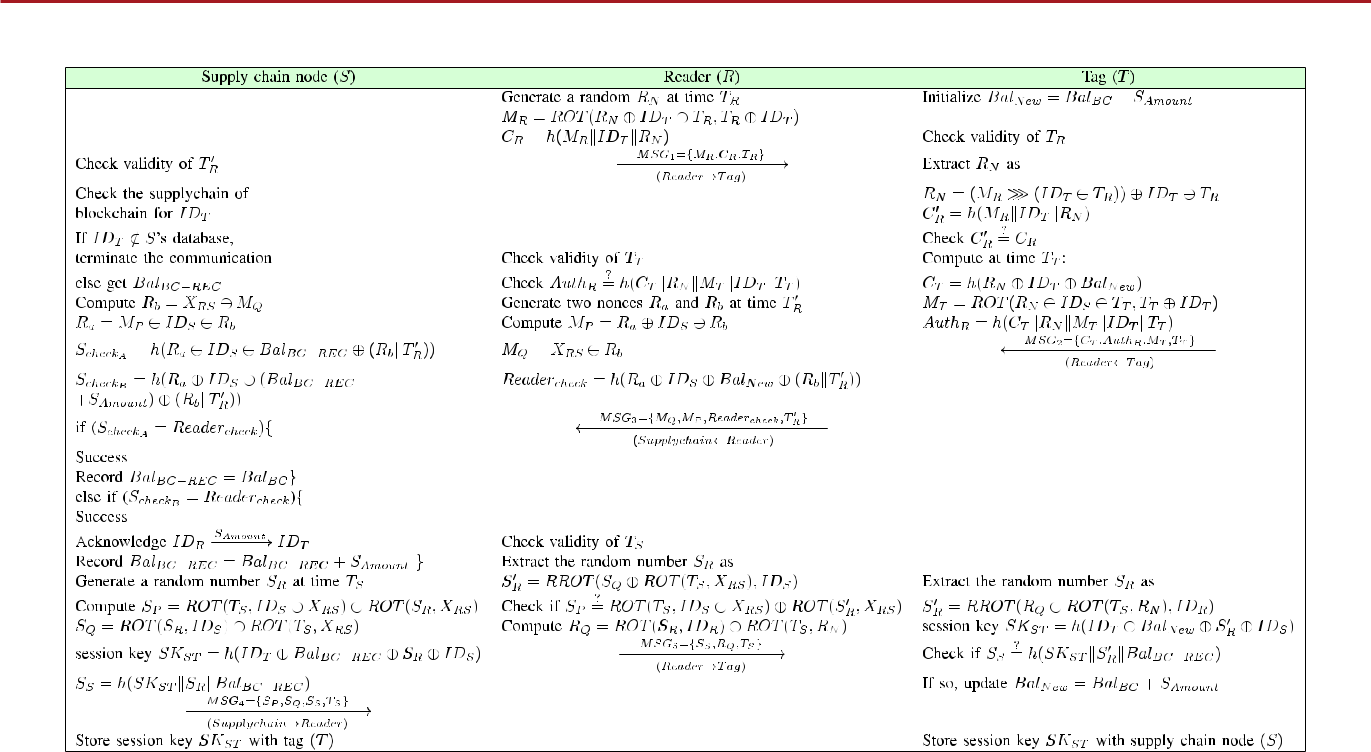


Fig. 6. Summary of mutual authentication and key agreement phase in LBRAPS.

If it passes, the reader (*R*) further computes *RQ* = *ROT* (*SR , IDR* )*⊕ ROT* (*TS , RN* )and transmits themessage *MSG*5 = *{SS* *, RQ* *, TS* *}* to the tag (*T* ) via open channel.

*Step 6:* The tag(*T* )receives the message *MSG*5from thereader (*R*) extracts the random number *SR* of the supply chain as *SR* = *RROT* (*RQ* *⊕ROT* (*TS* *, RN* )*,* *IDR* ), computes session key *SKS T* = *h*(*IDT ⊕ Bal*New *⊕SR ⊕IDS* )to authenticate both the supplychain node *S* and reader *R* by verifying the condition *SS* = *h*(*SKS T SR BalB C −*REC). If the verificationfails, the tag *T* refuses the communication. Otherwise, on successful authentication, the tag (*T* ) updates *Bal*New= *BalB C* + *S*Amountin its record and databasetoo.

After establishing the session key (*SKS T* = *h*(*IDT* *⊕* *Bal*New*⊕ SR ⊕ IDS* )) between the *T* and *S* with thehelp of the *R*, the blockchain balance is updated in the distributed ledger with new balance *Bal*New. The motivation for establishing the session key between the tag *T* and the supply chain node *S* is that depend-ing upon the future requirement the blockchain can intercept with the concerned department where the *T* and *S* want to communicate securely with the help of the established session key *SKS T* . It is worth noting that as illustrated in Sidorov *et al.*’s protocol [54], the practical scenarios of our mutual authentication protocol (LBRAPS) in blockchain-enabled supply chain can be also made easily in a similar way for various departments.

*Remark 1:* With the use of AI/machine learning (ML), datapoisoning has become a potential challenge as well as security

threat. This results in injecting false data by the fake users, and it leads to misleading training datasets with puzzling the AI/ML algorithms and also manipulating the trained models [57]. As a result, data poisoning can alter AI/ML algorithms and also produce wrong results, and it makes incorrect predictions. Thus, data losses and disruption because of data poisoning attacks lead to significant factor for businesses as well as organizations with respect to both financial terms and damaging their reputations. One of the methods to address the data poisoning attacks is to detect and remove the outliers from the available training datasets.

With the help of the proposed authentication scheme (LBRAPS), the data is securely brought back to the supply node(s) from the tag(s) by encrypting the data using the estab-lished session key *SKS T* . Then, the private blockchain is formed by the multiple departments of the supply nodes (see Fig. 5), and also multiple departments maintain a private blockchain together and perform the same authentication protocol process. Therefore, the transaction data stored in blockchain is authentic and genuine too. This helps in avoiding data poisoning attacks by an adversary, and it leads to run the AI/ML algorithms as per expectations in order to produce the correct predictions.

1. SECURITY ANALYSIS

This section shows that LBRAPS is resilient against several attacks, and also ensures user anonymity and untraceability.

*1) Confidentiality:* The messages *MSG*1= *{MR , CR , TR }*, *MSG*2= *{CT , AuthR , MT , TT }*, *MSG*3= *{MQ , MP , Reader*check*, TR }*, *MSG*4= *{SP , SQ , SS , TS }*, *MSG*5= *{SS , RQ , TS }* are related to the random numbers(*RN* , *Ra* , *Rb* , and *SR* )generated by the participants. It is difficult for

Authorized licensed use limited to: University of New South Wales. Downloaded on November 20,2020 at 02:19:00 UTC from IEEE Xplore. Restrictions apply.

?

= *ROT*(*TS* *,*

|  |  |
| --- | --- |
| JANGIRALA *et al.*: DESIGNING SECURE LIGHTWEIGHT BLOCKCHAIN-ENABLED RFID-BASED AUTHENTICATION | 7089 |
|  |  |

an attacker *A* to extract *RN* , *Ra* , *Rb* , and *SR* to compute the correct messages and also to make believe the other participants as authentic. Therefore, *A* cannot acquire the random numbers from the messages and impersonate the legitimate entities. Hence, the confidentiality of the transmitted data is preserved in LBRAPS.

1. *User Anonymity and Untraceability:* According to thethreat model discussed in Section II-B2, *A* can capture the messages *MSGj* , *j* = 1*,* 2*,* 3*,* 4*,* 5, which were communicated during the authentication and key agreement phase over the insecure channels. Without knowing the parametric values *IDR* , *IDT* , and *RN* , it is computationally infeasible task for *A* toguess the identities of both tag *T* and reader *R* in polynomial time. So, this ensures that *LBRAP S* holds the user anonymity property. In ensuring untraceability property, it is worth notic-ing that the messages *MSGj* (*i* = 1*,* 2*,* 3*,* 4*,* 5) are “dynamic” in nature which were computed using random numbers and current timestamps. Furthermore, due to the “noninvertible (collision-resistant) one-way property” of hash function *h*(*·*), it is computational task for *A* to trace the messages. Therefore, *A* can not keep track of the activities performed by the reader *R* and tag *T* over different sessions. Hence, LBRAPS also assures untraceability property.
2. *Mutual Authentication and Session Key Establishment:* Thereader *R*, the tag *T* , and the supply chain node *S* authenticate each other in LBRAPS. The message *MSG*1 = *{MR* *, CR* *, TR* *}* is protected by the secret random number *RN* and also the cur-rent time stamp *TR* . Only the legitimate *T* can acknowledge by

?

verifying if *CR* = *h*(*MR* *IDT* *RN* ). In the next step, *T* raises the challenge to the reader to authenticate the message *MSG*2 = *{CT , AuthR , MT , TT }* sent by *T* . The *R* then validates the

|  |  |  |  |
| --- | --- | --- | --- |
| message sent by the *T* | ? | *RN MT* |  |
| whether *AuthR* = *h*(*CT* |  |

*IDT TT* ). Now, *R* sends the message *MSG*3= *{MQ , MP , Reader*check*, TR }* to the *S*. On receiving the message, the *S* gen-erates its random number *SR* and the current timestamp *TS* , and computes the session key *SKS T* = *h*(*IDT* *⊕* *Bal*New*⊕* *SR* *⊕* *IDS* )to transmit the message *MSG*4= *{SP , SQ , SS , TS }*.Upon receiving the message from *S*, the *R* verifies the au-

thenticity of *S* by validating the message with *SP*

*IDS ⊕ XRS* )*⊕ ROT* (*SR , XRS* ). On successful verification, *R* authenticates *S* and transmits the message *MSG*5 = *{SS* *, RQ* *,* *TS }* to *T* . *T* extracts the random number *SR* of *R* and verifies the

?

authenticity of the message *MSG*5 sent by *R* as *SS* = *h*(*SKS T* *SR BalB C −*REC). If the verification is successful, both *T* and

1. are successful in establishing the session key *SKS T* and furthermore, all the participants are successful in verifying the authenticity of the sender and receiver parties. Thus, LBRAPS is successfull in preserving mutual authentication and ensuring the establishment of the session key.
   1. *Forward Secrecy:* If the tag *T* is compromised by anadversary *A*, the secret keys stored inside it are also leaked. *A* may then acquire the information transmitted in the previoussession. In LBRAPS, the random numbers and shared secret keys are not stored on the tag’s memory. Furthermore, the random numbers are generated freshly in every session for computing the session keys so that the session keys are distinct

in each session. Thus, compromising the session key or random numbers in a specific session do not lead to any advantage to *A*. Hence, LBRAPS ensures the forward secrecy.

1. *Internal Attacks:* Internal member may cheat other entitiesby impersonating other legal participants. Therefore, in our LBRAPS, there are two types of internal attacks, which are described below.

*a) Reader Impersonation Attack:* We consider that an internallegitimate reader of department 1 (*Dept*1) with the secret parameters tries to impersonate the other reader of *Dept*2 who owns the secret parameters that are different from *Dept*1. Now, when the forged reader queries the tag, the forge reader may send *MSG*1 to the legitimate tag which belongs to *Dept*2. The message *MSG*1 cannot be authenticated by the legitimate tag because the random numbers generated by the reader of *Dept*2 are different from those generated by the reader of *Dept*1. So, the tag cannot extract the correct random number *RN* and also cannot verify the authenticity of the message *MSG*1. Thus, the reader impersonation attack is restricted in LBRAPS.

*b) Tag Impersonation Attack:* We also consider that an internallegitimate tag of *Dept*1 with the secret parameters tries to impersonate the other tag of another *Dept*2 who owns the secret parameters that are different from *Dept*1. When the forged tag queries the reader, the forged tag sends *MSG*2 to the legitimate reader which belongs to *Dept*2. The message *MSG*2 cannot be authenticated by the legitimate reader because the random numbers generated by the tag of *Dept*2 are different from those generated by the tag of *Dept*1. This means that the reader cannot verify the authenticity of *MSG*2 by checking the

?

condition *AuthR* = *h*(*CT* *RN MT IDT TT* ). Thus, thetag impersonation attack is also restricted in LBRAPS.

1. *External Attacks:* We consider the following two activeattacks.

*a) Replay Attack:* We consider that during the authenticationand key agreement phase, *A* tries to intercept the messages *MSGj* , *j ∈* [1*,* 5]to frame replay attack by replaying these mes-sages to the receiver. But this attempt fails due to the involvement of the current timestamps and random numbers embedded in the communicated messages *MSGj* , *j* *∈* [1*,* 5]. Upon receiving the messages, the initial step is the timestamp verification and then for the validation of the transmitted messages. Thus, framing the replay attack is resisted in LBRAPS.

*b) Man-in-the-Middle Attack:* During the authentication andkey agreement phase, suppose *A* wishes to capture and modify the messages *MSGj* , *j* *∈* [1*,* 5] to believe the participants that the messages received from the genuine authentic participants. To frame this attack, suppose *A* wants to modify the message *MSG*1. But, this attempt fails due to the lack of knowledgeon the involved secret *RN* . Similarly, *A*’s attempts also fail to modify the other messages: *MSG*2 for random secret *RN* ; *MSG*3for random secrets *Ra* & *Rb* ; *MSG*4for random secrets *SR* ; and *MSG*5for random secret *SR* . Thus, due to randomnessof the messages and usage of current timestamps, LBRAPS withstands the “man-in-the-middle attack.”

1. *Ephemeral Secret Leakage (ESL) Attack:* During theauthentication and key agreement phase, after validating mutual authentication as shown above, both the supply chain node *S* and

Authorized licensed use limited to: University of New South Wales. Downloaded on November 20,2020 at 02:19:00 UTC from IEEE Xplore. Restrictions apply.

7090 IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 16, NO. 11, NOVEMBER 2020

the tag *T* establish a common session key *SKS T* . According to the discussed threat model in Section II-B2, we consider the current *de facto* CK-adversary model for the session key (SK)-security. The reliability of SK-security in LBRAPS is relied on the following two cases.

*Case 1:* Assume the ephemeral (short term) secrets *RN , Ra , Rb* , and *SR* are some how known to an adversary *A*.The challenge for *A* is to create the session key *SKS T* based on the short-term secrets. But, due to the lack of knowledge of long-term secrets (*IDT* , *IDS* , *XRS* , *IDR* , *BalB C* , and *S*Amount),

* fails to succeed in its challenge as it is “computationally infeasible task” for *A* to guess the long-term secrets.

*Case 2:* Suppose few or all of the long-term secrets (*IDT* , *IDS* , *XRS* , *IDR* , *BalB C* , and *S*Amount) are some how leakedto *A*. Now, the similar challenge for *A* as in Case 1 remains to construct *SKS T* . However, without knowledge of short-term secrets (*RN* *, Ra* *, Rb* , and *SR* ), it is also “computationally in-feasible task” for *A* to win the challenge by guessing only the short-term secrets.

From the above two cases, it is clear that the valid session key *SKS T* is only computed with legitimate long-term secrets alongwith short-term secrets, which is possible only by the legitimate participants (*S, R,* and *T* ). Furthermore, in LBRAPS, compro-mising of current session key does not lead to compromise the previous and future sessions as the session keys are randoms and unique in each session. Therefore, *A* can not determine the previous and future session keys even if the current session key is compromised [58]. Thus, LBRAPS successfully preserves both backward and forward secrecy along with the SK-security. Even with the help of some session hijacking attacks, only a particular session key can be leaked. But, its effect does not compromise the previous and future sessions. Hence, LBRAPS is secure against ESL attack.

VI. FORMAL SECURITY VERIFICATION USING AVISPA:

SIMULATION STUDY

We apply the broadly accepted formal security software ver-ification tool, called AVISPA [59] for validating the security of our proposed LBRAPS against an adversary. The “High-Level Protocol Specification Language (HLPSL)” in AVISPA is used to implement a security protocol in order to test whether the designed protocol is safe or unsafe using one of the four backends, namely “On-the-fly Model-Checker (OFMC),” “Con-straint Logic based-Attack Searcher (CL-AtSe),” “SAT-based Model-Checker (SATMC),” and “Tree Automata based on Au-tomatic Approximations for the Analysis of Security Protocols (TA4SP).” The HLPSL code is transferred into the “Intermediate Format (IF).” The IF is then supplied as input to one of the four backends, which leads to produce the “Output Format (OF).” The OF has various sections as described in [59]. More details about AVISPA as well as HLPSL implementation can be found in [59].

In our implementation, we have basic and composite roles. The basic roles represent various participants in the protocol (the roles for the reader, tag, and supply chain node). However, the composition roles, which are mandatory roles (session

Fig. 7. Analysis of simulation results under OFMC and CL-AtSe backends.

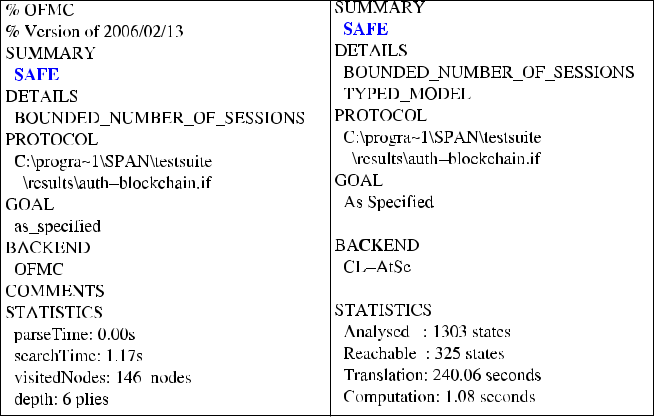
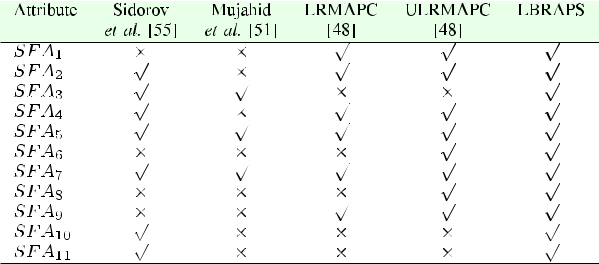


TABLE II

COMPARISON OF SECURITY AND FUNCTIONALITY FEATURES



*√*

* a scheme supports an attribute or resists an attack; *×*: a scheme does not support an attribute or it does not resist an attack.

*S F A*1: privileged-insider attack; *S F A*2: anonymity; *S F A*3: traceability;

*S F A*4: denial-of-service attack; *S F A*5: mutual authentication; *S F A*6: ESL

attack; *S F A*7 : replay attack; *S F A*8 : impersonation attacks; *S F A*9 : man-in-the-

middle attack; *S F A*10 : formal security verification using AVISPA tool; *S F A*11 :

whether blockchain-enabled.

and goal and environment), are various scenarios involving basic roles. The broadly accepted “SPAN (Security Protocol ANimator for AVISPA)” tool [60] is applied to perform formal security verification part through simulation on our LBRAPS. The simulation results shown in Fig. 7 assure that LBRAPS protects both replay and man-in-the-middle attacks.

VII. PERFORMANCE COMPARISON

We perform a rigorous comparative study on security and functionality features, computation and communication costs during the authentication and key agreement phase among the proposed LBRAPS and the existing schemes of Sidorov *et al.* [54], Mujahid *et al.* [50], and Fan *et al.* [47].

1. *Comparison of Security and Functionality Features:* InTable II, LBRAPS is compared with the earlier schemes of Sidorov *et al.* [54], Mujahid *et al.* [50] and Fan *et al.* [47]

based on several security and functionality features *SF Ai* (*i* = 1*,* 2*, . . . ,* 11). LRMAPC protocol proposed by Fan *et al.*

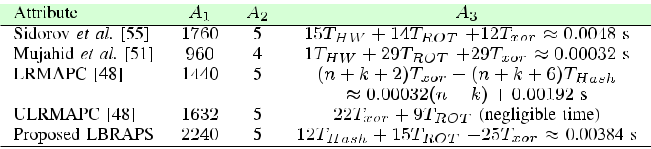
1. fails to achieve reader impersonation, tag forgery, and message eavesdropping attacks [48]. In addition, it does not provide untracebility property and is not resilient against

Authorized licensed use limited to: University of New South Wales. Downloaded on November 20,2020 at 02:19:00 UTC from IEEE Xplore. Restrictions apply.

|  |  |
| --- | --- |
| JANGIRALA *et al.*: DESIGNING SECURE LIGHTWEIGHT BLOCKCHAIN-ENABLED RFID-BASED AUTHENTICATION | 7091 |
|  |  |

TABLE III

COMPARISON OF COMMUNICATION AND COMPUTATION COSTS



1. 1 : communication cost in bits; *A*2 : number of exchanged message; *A*3 : computation cost with rough estimated time in seconds.

ESL attack. Furthermore, ULRMAPC protocol proposed by Fan *et al.* [47] does not also provide untraceability property. It is worth noticing that the scheme of Mujahid *et al.* [50], LRMAPC and ULRMAPC are not blockchain-enabled. As a result, LBRAPS supports more functionality features and also provides better security features as compared to those for other schemes.

1. *Comparison of Communication Costs:* We consider thathash output is 160 bits (if SHA-1 hash function [61] is applied), humming weight is 160 bits, identities and random numbers are 160 bits, and timestamp is 32 bits. In the protocols of Sidorov *et al.* [54] and Mujahid *et al.* [50], the “Hello” message isconsidered as 160 bits. In Fan *et al.*’s two protocols, namely LRMAPC [47] and ULRMAPC [47], it is assumed that “Query” is of 160 bits. In our LBRAPS, the messages *MSG*1, *MSG*2, *MSG*3, *MSG*4, and *MSG*5need(160+160+32) =352 bits,(160+ 160+ 160+ 32) = 512 bits, (160+ 160+ 160+ 32) = 512 bits, (160+ 160+ 160+ 32) = 512 bits, and (160+ 160+ 32) = 352 bits, respectively. Therefore, the total communication cost required in LBRAPS due to exchange of five messages is 2240 bits. We then compare the communication cost of LBRAPS with other schemes in Table III. It is observed that the proposed LBRAPS needs more communication cost as compared to other schemes. However, our LBRAPS is the only scheme which is able to protect RFID systems from possible potential security attacks. In addition, LBRAPS outperforms other existing protocols, and LBRAPS and Sidorov *et al.*’s scheme [54] are the protocols that were designed to be integrated into the blockchain whereas Mujahid *et al.*’s scheme [50] and other two protocols: LRMAPC [47] and ULRMAPC [47] are not designed for blockchain. Moreover, in Mujahid *et al.*’s scheme and ULRMAPC [47], no session key is established between the entities.
2. *Comparison of Computation Costs:* Let *T*xor, *TH W* , *T*Hash,and *T*ROT denote the time needed for executing an exclusive-OR, Hamming weight, one-way hash function, and left/right rotation operations, respectively. It is assumed that *T*Hash *≈* *TH W* *≈* 0*.*00032 s [58]. As *T*ROT and *T*xor are negligible in computation, these are ignored in computation. In LRMAPC [47], *n* and *k* denote the number of keys in the cache and the number of keys in the database, respectively. During the authentication and key agreement phase of LBRAPS, an RFID tag requires the computational cost of 5*T*Hash + 4*T*ROT, while a reader needs

the computational cost of 3*T*Hash + 7*T*ROT and the supply chain node demands the computational cost of 4*T*Hash + 4*T*ROT for the supplychain of blockchain data update process. Therefore,

the total computation cost of LBRAPS is 12*T*Hash + 15*T*ROT. From the comparative study on computational costs among the schemes presented in Table III, LBRAPS needs less cost than Sidorov *et al.*’s scheme [54]. Though Mujahid *et al.*’s scheme [50] needs less cost than both LBRAPS and Sidorov *et al.*’s scheme, no session key is established between the entitiesin [50] and it fails to support all functionality and security features (see Table II). Moreover, though ULRMAPC [47] needs minimum computation cost as compared to all other schemes including the proposed LBRAPS, it also fails to fulfill all functionality and security features (see Table II).

VIII. CONCLUSION

This article handled an important problem related to blockchain-enabled RFID-based authentication for supply chains in 5G mobile edge computing environment. We pro-posed an efficient authentication protocol (LBRAPS), which is not only efficient in both communication and computation but also supported many security and functionality features. Various potential attacks were protected in LBRAPS. The AVISPA-based simulation on the formal security verification also proved that LBRAPS was secured against active attacks. Moreover, LBRAPS had better tradeoff among security as well as functionality features, and communication and computational costs as compared to other schemes which were demonstrated in Tables II and III. In the future, we target to implement the proposed scheme (LBRAPS) in a real-world environment.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and Associate Editor for their valuable feedback on this article.

REFERENCES

1. J. N. Dewey, R. Hill, and R. Plasencia, “Blockchain and 5G-Enabled Internet of Things (IoT) will redefine Supply Chains and Trade Finance,” Accessed: Feb. 2019. [Online]. Available: [https://www.hklaw.com/files/](https://www.hklaw.com/files/Uploads/Documents/Articles/Blockchain5GEnabledInternetofThings.pdf) [Uploads/Documents/Articles/Blockchain5GEnabledInternetofThings.pdf](https://www.hklaw.com/files/Uploads/Documents/Articles/Blockchain5GEnabledInternetofThings.pdf)
2. S. Yi, C. Li, and Q. Li, “A survey of fog computing: Concepts, applications and issues,” in *Proc. Workshop Mobile Big Data*, Hangzhou, China, 2015, pp. 37–42.
3. Y. Ai, M. Peng, and K. Zhang, “Edge computing technologies for Internet of Things: A primer,” *Digit. Commun. Netw.*, vol. 4, no. 2, pp. 77–86, 2018.
4. M. A. Rahman *et al.*, “Blockchain-based mobile edge computing frame-work for secure therapy applications,” *IEEE Access*, vol. 6, pp. 72 469– 72 478, 2018.
5. B. Whittle, “The Implications of Fusing 5 G and Blockchain.” Accessed: Apr. 2019. [Online]. Available: <https://cointelegraph.com/news/the-implications-of-fusing-5g-and-blockchain>
6. Blockchain Institute, “How Blockchain can impact the telecommunica-tions industry and its relevance to the C-Suite,” Accessed: Jan. 2019. [Online]. Available: [https://www2.deloitte.com/content/dam/Deloitte/za/](https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/za_TMT_Blockchain_TelCo.pdf) [Documents/technology-media-telecommunications/za\_TMT\_Blockchain](https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/za_TMT_Blockchain_TelCo.pdf) [\_TelCo.pdf](https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/za_TMT_Blockchain_TelCo.pdf)
7. H. Min, “Blockchain technology for enhancing supply chain resilience,” *Bus. Horizons*, vol. 62, no. 1, pp. 35–45, 2019.
8. J. W. Michael, A. Cohn, and J. R. Butcher, “BlockChain technology,” *The* *J.*, 2018.
9. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in *Proc. IEEE Int. Congr. Big Data*, Honolulu, HI, USA, 2017, pp. 557–564.

Authorized licensed use limited to: University of New South Wales. Downloaded on November 20,2020 at 02:19:00 UTC from IEEE Xplore. Restrictions apply.

7092 IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 16, NO. 11, NOVEMBER 2020

1. T. Aste, P. Tasca, and T. Di Matteo, “Blockchain technologies: The foreseeable impact on society and industry,” *IEEE Comput.*, vol. 50, no. 9,
   1. 18–28, 2017.
2. D. Ongaro and J. Ousterhout, “In search of an understandable consensus algorithm,” in *Proc. USENIX Annu. Tech. Conf.*, Philadelphia, PA, USA, 2014, pp. 305–319.
3. R. Khaitan, “Blockchain: One Truth Across Networks for the Sup-

ply Chain,” [Online]. Available: [https://www.ibm.com/blogs/watson-customer-engagement/2017/04/11/blockchain-supply-chain/.](https://www.ibm.com/blogs/watson-customer-engagement/2017/04/11/blockchain-supply-chain/) Accessed: Apr. 2019.

1. Cibusworld, “Cibus Blockchain will transform the global food supply chain,” [Online]. Available: [https://coins.newbium.com/post/14642-cibus](https://coins.newbium.com/post/14642-cibus-blockchain-will-transform-the-global-food-su) [-blockchain-will-transform-the-global-food-su.](https://coins.newbium.com/post/14642-cibus-blockchain-will-transform-the-global-food-su) Accessed: Feb. 2017.
2. Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, “When mobile blockchain meets edge computing,” *IEEE Commun. Mag.*, vol. 56, no. 8,
   1. 33–39, Aug. 2018.
3. K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, “Blockchain for AI: Review and open research challenges,” *IEEE Access*, vol. 7, pp. 10 127–10 149, Jan. 2019.
4. H.-C. Hsieh, J.-L. Chen, and A. Benslimane, “5G virtualized multi-access edge computing platform for IoT applications,” *J. Netw. Comput. Appl.*, vol. 115, pp. 94–102, 2018.
5. Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, “Mobile edge computing-A key technology towards 5G,” Sophia Antipolis, France, ETSI, White Paper no. 11, pp. 1–16, 2015.
6. K. Peng, V. Leung, X. Xu, L. Zheng, J. Wang, and Q. Huang, “A survey on mobile edge computing: Focusing on service adoption and provision,” *Wireless Commun. Mobile Comput.*, vol. 2018, 2018, Art. no. 8267838.
7. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future* *Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.
8. X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, “A robust ECC-based provable secure authentication protocol with privacy protection for industrial internet of things,” *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3599–3609, Aug. 2018.
9. S. Dhanani, “Industrial Internet of Things (IIoT) and Its Impact on the Design of Automation Systems,” 2017. Accessed: Apr. 2017. 2019. [Online]. Available: [https://www.maximintegrated.com/en/app-notes/](https://www.maximintegrated.com/en/app-notes/index.mvp/id/6142) [index.mvp/id/6142](https://www.maximintegrated.com/en/app-notes/index.mvp/id/6142)
10. L. D. Xu, W. He, and S. Li, “Internet of things in industries: A survey,” *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.
11. M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, “Design of secure user authenticated key management protocol for generic IoT networks,” *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018.
12. Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the Internet of Things: perspectives and challenges,” *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, 2014.
13. “Watson IoT Platform,” IBM. Accessed: July 2019. [Online]. Available: <https://www.ibm.com/internet-of-things/solutions/iot-platform>
14. C. Hsu and W. A. Wallace, “An industrial network flow informa-tion integration model for supply chain management and intelligent transportation,” *Enterprise Inf. Syst.*, vol. 1, no. 3, pp. 327–351, 2007.
15. “Nebula AI (NBAI) – Decentralized AI Blockchain Whitepa-per,” 2018, Nebula AI Team. [Online]. Available: [https://neironix.io/](https://neironix.io/documents/whitepaper/4082/NBAI_whitepaper_EN.pdf) [documents/whitepaper/4082/NBAI\_whitepaper\_EN.pdf.](https://neironix.io/documents/whitepaper/4082/NBAI_whitepaper_EN.pdf) Accessed: Jul. 2019.
16. T. N. Dinh and M. T. Thai, “AI and Blockchain: A Disruptive Integration,” *Computer*, vol. 51, no. 9, pp. 48–53, 2018.
17. G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” *Ethereum Project Yellow Paper*, vol. 151, no. 2014, pp. 1–32, 2014.
18. M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed. Boston, MA,

USA: O’Reilly Media, 2015.

1. T. Marwala and B. Xing, “Blockchain and Artificial Intelligence,” 2018, *arXiv preprint arXiv:1802.04451*.
2. “Supply Chain Solutions,” 2019, GlobalTranz, Phoenix, AZ, USA. Accessed: Aug. 2019. [Online]. Available: [https://www.globaltranz.](https://www.globaltranz.com/shippers/supply-chain-solutions/) [com/shippers/supply-chain-solutions/](https://www.globaltranz.com/shippers/supply-chain-solutions/)
3. Kamesh, “Why supply chains need Blockchain solutions more than ever.” Accessed: March 2019. [Online]. Available: [https://medium.com/](https://medium.com/@kwrdarisipudi/why-supply-chains-need-blockchain-solutions-more-than-ever-93206ae7f9dd) [@kwrdarisipudi/why-supply-chains-need-blockchain-solutions-more-than-ever-93206ae7f9dd](https://medium.com/@kwrdarisipudi/why-supply-chains-need-blockchain-solutions-more-than-ever-93206ae7f9dd)
4. Yuz, “Waltonchain.” Accessed: Jun. 2018. [Online]. Available: [https://](https://steemit.com/cryptocurrency/@yuz/what-is-waltonchain-wtc) [steemit.com/cryptocurrency/@yuz/what-is-waltonchain-wtc](https://steemit.com/cryptocurrency/@yuz/what-is-waltonchain-wtc)
5. S. Wang, S. Zhu, and Y. Zhang, “Blockchain-based mutual authentication security protocol for distributed RFID systems,” in *Proc. IEEE Symp.* *Comput. Commun.*, Natal, Brazil, 2018, pp. 74–77.
6. D. Dolev and A. Yao, “On the security of public key protocols,” *IEEE* *Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
7. R. Canetti and H. Krawczyk, “Universally composable notions of key exchange and secure channels,” in *Proc. Int. Conf. Theory Appl. Cryp-tographic Techn.– Advances Cryptology*, Amsterdam, The Netherlands,2002, pp. 337–351.
8. D. He, N. Kumar, N. Chilamkurti, and J.-H. Lee, “Lightweight ECC Based RFID authentication integrated with an ID verifier transfer protocol,” *J.* *Med. Syst.*, vol. 38, no. 10, 2014, Art. no. 116.
9. C.-I. Lee and H.-Y. Chien, “An elliptic curve cryptography-based RFID authentication securing E-Health system,” *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 12, pp. 1–7, 2015.
10. Y.-P. Liao and C.-M. Hsiao, “A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol,” *Ad Hoc Netw.*, vol. 18, pp. 133–146, 2014.
11. N. Li, Y. Mu, W. Susilo, F. Guo, and V. Varadharajan, “Vulnerabilities of an ECC-based RFID authentication scheme,” *Security and Commun.* *Netw.*, vol. 8, no. 17, pp. 3262–3270, 2015.
12. D. He and S. Zeadally, “An analysis of RFID authentication schemes for Internet of Things in healthcare environment using elliptic curve cryptography,” *IEEE Internet Things J.*, vol. 2, no. 1, pp. 72–83, Feb. 2015.
13. X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K. R. Choo, “A robust and energy efficient authentication protocol for industrial internet of things,” *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1606–1615, Jun. 2018.
14. X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, and C. Chen, “A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems,” *IEEE Syst. J.*, pp. 1–12, 2019, doi: [10.1109/JSYST.2019.2899580](https://dx.doi.org/10.1109/JSYST.2019.2899580).
15. X. Li, S. Liu, F. Wu, S. Kumari, and J. J. P. C. Rodrigues, “Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications,” *IEEE Internet Things J.*, vol. 6, no. 3, Jun. 2019.
16. C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, “BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0,” *J. Netw. Comput. Appl.*, vol. 116, pp. 42–52, Aug. 2018.
17. K. Fan, Y. Gong, C. Liang, H. Li, and Y. Yang, “Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G,” *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3095–3104, 2016.
18. C. T. Li, C. C. Lee, C. Y. Weng, and C. M. Chen, “Towards secure authenticating of cache in the reader for RFID-based IoT systems,” *Peer-to-Peer Netw. Appl.*, vol. 11, no. 1, pp. 198–208, 2018.
19. K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, “A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain,” *IEEE Access*, vol. 5, pp. 17 465– 17 477, 2017.
20. U. Mujahid, M. Najam-ul Islam, and S. Sarwar, “A new ultralightweight RFID authentication protocol for passive low cost tags: KMAP,” *Wireless* *Pers. Commun.*, vol. 94, no. 3, pp. 725–744, 2017.
21. *EPC*T M *Radio-Frequency Identity Protocols Generation-2 UHF RFID*,Specification for RFID Air Interface Protocol for Communications at 860 MHz – 960 MHz, Version 2.0.1 Ratified, 2013.
22. J. Ha, H. Kim, J. Park, S. Moon, J. G. Nieto, and C. Boyd, “HGLAP– Hierarchical Group-Index Based Lightweight Authentication Protocol for Distributed RFID System,” in *Proc. Int. Conf. Embedded Ubiquitous* *Comput.*, Taipei, Taiwan, 2007, pp. 557–567.
23. K. Rhee, J. Kwak, S. Kim, and D. Won, “Challenge-response based RFID authentication protocol for distributed database environment,” in *Proc. Int.* *Conf. Secur. Pervasive Comput.*, Boppard, Germany, 2005, pp. 70–84.
24. M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura, and J. H. Khor, “Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains,” *IEEE Access*, vol. 7, pp. 7273–7285, 2019.
25. M. Safkhani and M. Shariat, “Implementation of secret disclosure attack against two IoT lightweight authentication protocols,” *J. Supercomputing*, vol. 74, no. 11, pp. 6220–6235, 2018.
26. A. Litke, D. Anagnostopoulos, and T. Varvarigou, “Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment,” *Logistics*, vol. 3, no. 1, 2019.
27. X. Chen, C. Liu, B. Li, K. Lu, and D. Song, “Targeted backdoor attacks on deep learning systems using data poisoning,” *CoRR*, vol. abs/1712.05526, 2017. [Online]. Available: <http://arxiv.org/abs/1712.05526>

Authorized licensed use limited to: University of New South Wales. Downloaded on November 20,2020 at 02:19:00 UTC from IEEE Xplore. Restrictions apply.

|  |  |
| --- | --- |
| JANGIRALA *et al.*: DESIGNING SECURE LIGHTWEIGHT BLOCKCHAIN-ENABLED RFID-BASED AUTHENTICATION | 7093 |
|  |  |

1. J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, “Cloud centric authentication for wearable healthcare monitoring system,” *IEEE Trans. Dependable Secure Comput.*, to be published, 2018,doi: [10.1109/TDSC.2018.2828306](https://dx.doi.org/10.1109/TDSC.2018.2828306).
2. AVISPA, “Automated Validation of Internet Security Protocols and Applications,” 2019. Accessed: Feb. 2019. [Online]. Available: <http://www.avispa-project.org/>
3. AVISPA, “SPAN, the Security Protocol ANimator for AVISPA,” 2019. Accessed: Feb. 2019. [Online]. Available: <http://www.avispa-project.org/>
4. *Secure Hash Standard*, FIPS PUB 180-1, National Institute of Stan-dards and Technology (NIST), U.S. Department of Commerce, April 1995. Accessed: Feb. 2019. [Online]. Available: [http://nvlpubs.nist.](http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf) [gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf](http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf)

**Srinivas Jangirala** (M’19) received the B.Sc.and M.Sc. degrees in mathematics from Kakatiya University, Telangana, India, in 2003 and 2008, respectively, the M.Tech. degree in computer science and data processing from Indian Institute of Technology (IIT) Kharagpur, Kharagpur, India, in 2011, and the Ph.D. degree in cryptography from the Department of Mathe-matics, IIT Kharagpur, in 2017.



He is currently working as an Assistant Profes-sor of Computer Science and Engineering with Jindal Global Business School, O. P. Jindal Global University, Haryana,

India. Prior to this, he also worked as a Research Assistant with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology (IIIT), Hyderabad, India. He has authored 16 papers in international journals and conferences in his research areas. His research interests include authentication protocols, information security, digital rights management, and cloud computing.

**Ashok Kumar Das** (M’17–SM’18) received theM.Sc. degree in mathematics, the M.Tech. de-gree in computer science and data processing, and the Ph.D. degree in computer science and engineering, from Indian Institute of Technology (IIT) Kharagpur, Kharagpur, India, in 1998, 2000, and 2009, respectively.



He is currently an Associate Professor of Computer Science and Engineering with the Center for Security, Theory and Algorithmic Research, International Institute of Information

Technology (IIIT), Hyderabad, India. He has authored over 195 papers in international journals and conferences in the above areas, including over 170 reputed journal papers. His current research interests include cryptography and network security including security in smart grid, Inter-net of Things (IoT), Internet of Drones (IoD), Internet of Vehicles (IoV), cyber-physical systems (CPS) and cloud computing, and blockchain.

Dr. Das is on the Editorial Board of *Korean Society for Internet* *Information (KSII) Transactions on Internet and Information Systems*, *International Journal of Internet Technology and Secured Transactions* (Inderscience), and *Institution of Engineering and Technology (IET)* *Communications*. He was a recipient of the Institute Silver Medal fromIIT Kharagpur.

**Athanasios V. Vasilakos** (SM’09) received thePh.D. degree in computer engineering from the University of Patras, Patras, Greece, in 1988.



He is currently a Professor with the Depart-ment of Computer Science, Electrical and Com-puter Engineering, Lulea˚ University of Technol-ogy, Lulea,˚ Sweden and also with the Com-puter Science and Technology, Fuzhou Univer-sity, Fuzhou, China. He has published over 700 technical research papers in leading journals and conferences in his areas of research.

Mr. Vasilakos served or is serving as an Editor for many technical journals, such as the IEEE TRANSACTIONS ON NETWORK AND SER-

VICE MANAGEMENT, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANS-ACTIONS ON CYBERNETICS, IEEE TRANSACTIONS ON NANOBIOSCIENCE, IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE COMMUNICATION MAGAZINE, ACM TRANSACTIONS ON AUTONOMOUS AND ADAPTIVE SYSTEMS, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, ACM TRANSACTIONS ON AUTONOMOUS AND ADAPTIVE SYSTEMS, etc. He was awarded as a Highly Cited Researcher by Web of Science in 2017 and 2018. He is also the General Chair of the European Alliances for Innovation.

Authorized licensed use limited to: University of New South Wales. Downloaded on November 20,2020 at 02:19:00 UTC from IEEE Xplore. Restrictions apply.