sensors

MDPI

Article

A Hash-Based RFID Authentication Mechanism for Context-Aware Management in IoT-Based Multimedia Systems

Deebak B D [1,*], Fadi Al-Turjman [2] and Leonardo Mostarda [3]

1 Schoool of Computer Science and Engineering, Vellore Institute of Technology, Vellore-632014, India
2 Computer Engineering Department, Antalya Bilim University, 07190-Antalya, Turkey
3 Computer Science Department, Camerino University, 62032-Camerino, Italy
* Correspondence: deebak.bd@vit.ac.in

Received: 5 July 2019; Accepted: 9 August 2019; Published: 4 September 2019

Abstract: With the technological advances in the areas of Machine-To-Machine (M2M) and Device-To-Device (D2D) communication, various smart computing devices now integrate a set of multimedia sensors such as accelerometers, barometers, cameras, fingerprint sensors, gestures, iris scanners, etc., to infer the environmental status. These devices are generally identified using radio-frequency identification (RFID) to transfer the collected data to other local or remote objects over a geographical location. To enable automatic data collection and transition, a valid RFID embedded object is highly recommended. It is used to authorize the devices at various communication phases. In smart application devices, RFID-based authentication is enabled to provide short-range operation. On the other hand, it does not require the communication device to be in line-of-sight to gain server access like bar-code systems. However, in existing authentication schemes, an adversary may capture private user data to create a forgery problem. Also, another issue is the high computation cost. Thus, several studies have addressed the usage of context-aware authentication schemes for multimedia device management systems. The security objective is to determine the user authenticity in order to withhold the eavesdropping and tracing. Lately, RFID has played a significant for the context-aware sensor management systems (CASMS) as it can reduce the complexity of the sensor systems, it can be available in access control, sensor monitoring, real time inventory and security-aware management systems. Lately, this technology has opened up its wings for CASMS, where the challenging issues are tag-anonymity, mutual authentication and untraceability. Thus, this paper proposes a secure hash-based RFID mechanism for CASMS. This proposed protocol is based on the hash operation with the synchronized secret session-key to withstand any attacks, such as desynchronization, replay and man-in-the-middle. Importantly, the security and performance analysis proves that the proposed hash-based protocol achieves better security and performance efficiencies than other related schemes. From the simulation results, it is observed that the proposed scheme is secure, robust and less expensive while achieving better communication metrics such as packet delivery ratio, end-to-end delay and throughput rate.

Keywords: multimedia device management systems; RFID; context aware sensor management systems; replay; de-synchronization; traceability

1. Introduction

In the recent past, the development of smart computing devices in the Internet of Things (IoT) has grown exponentially [1,2]. These devices share the geo-location of physical objects with other systems. They are widely used in smart infrastructure to build the smart city features such as smart eHealthcare,

finance, e-Governance, parking and transportation [3]. There are more physical objects involved in connecting IoT-based applications in smart infrastructure. This infrastructure often integrates radio frequency identification (RFID) to configure different application environments such as smart inventory, toll-booth collection, object identification, anti-counterfeit protection and the automobile industries [4]. In contrast to bar-coding systems, the physical objects equipped with an RFID tag are not required to be in line-of-sight to read the encapsulated data. As a result, a long-sighted RFID-tag position can easily extract a large amount of RFID information to replace traditional supply-chain management systems with an RFID-based authentication system. Besides, the real-time objects track and identify the RFID information wirelessly to automate communication systems. It is considered as a promising technology to monitor the smart objects.

The technology known as Radio Frequency Identification (RFID) reads the physical objects and automatically recognizes the relative object details, i.e., it is basically a non-contract recognition technique [5]. This technique uses some type of artificial inference to sense the radio frequency that provides a communication between the tags attaching with the objects and the readers connecting with the backend server systems. Using this technology, several application systems such as chain management, credit-card, electronic passport verification, vehicle systems (i.e., charging and keyless entry), etc. have been designed and developed. Specifically, the countries like Japan, USA and other developing countries are nowadays becoming equipped with advanced RFID systems [6]. Lately, it has undergone further advancement in the form of electric induction [7] that recognizes the tag attachment object to read the object information.

RFID tags do not need any light source to sense the data through external materials, which makes them durable, low-cost, reliable and secure in comparison with bar-code systems [8]. Most retailers have employed this technology for integration of tag attachments that allow an authorized dealership to deliver the goods. For instance, Wal-Mart imbeds RFID tags in products which reduces the manpower and the materials resource needed by producers [9]. Moreover, this technology is now considered to be an integral part of people's daily activities such as the use of cellphones, automobiles, household objects, etc. It does not need any physical contact to sense or scan different types of objects. Importantly, it uses one signal to scan the various types of barcodes and in addition it has an ability to read and write tags multiple times [10]. This technology can even be used in different climate conditions like snow, fog and in packaging [11].

It is perceived to be a significant advancement for the development of future markets. Most of the enterprises and manufacturing industries including governments, banking, transportation, agriculture, food safety, healthcare, etc. are attaching these tags to automate the product delivery process faster in order to improve customer service and business automation efficiency. In the past, the usage of RFID, specifically in the range of high-frequency (HF-13.56 MHz) has gained much attention. Particularly, the Near Field Communication (NFC) standard has been designed and improved for the five types of NFC's i.e., in correspondence with different types of ISO/IEC and JIS standards. In general, the type 1, 2 and 4 are overlaid for ISO/IEC 14443-A, whereas the type 3 and 5 are dealt with in JIS X6319 and ISO/IEC 15693 (18000-3), respectively [12]. New manufacturers like NXP Semiconductor (Newburyport, MA, USA) have advanced the use of NFC technology, i.e., ntag-213/215/216. NFC cards are used in access control to improve the enterprise security.

Smartphone usage has developed exponentially in the past few years. As referred in [13], the number of smartphones used worldwide is predicted to be 4.49 billion (i.e., 59.9% of the global population). This generalization demands high user-level confidentiality to ensure security and privacy. In the USA [14] and EU [15], national program and strategies have intensified researchers' attention in support of privacy. Recently, the computation power of programmable smartcards has increased tremendously for the massive development of smart electronic devices such as public transportation, e-passports, e-ticketing and e-identification. These RFID-based communication devices are expected to provide tag anonymity in order to ensure privacy enhancement. Due to security and

privacy issues, RFID-based authentication schemes are gradually becoming assimilated in several real-time applications.

Generally speaking, RFID manages to track the unauthorized client access to ensure the privacy of RFID tags to resist potential vulnerabilities. Due to their limited computation resources, power and storage capabilities, it is more complicated to apply the expensive cryptographic operations in low-power RFID systems. Moreover, the expensive computations have slowed the development of RFID technologies [16–18]. Most significantly, adoptive RFID technologies cannot properly exploit the authentication process to enhance their security-level. In order to restrict malicious activities, the source messages should be prevented from fake broadcasting. It is noted that the physical security of RFID tags should be proactively secured to prevent unauthorized access. Moreover, the attackers then would not be able to track the previous user tag information to impersonate a legitimate user. Thus, this paper introduces a novel hash-based RFID mechanism using synchronized secret session key value and its objective is to: (1) Provide user privacy; (2) Reduce the power consumption; (3) Reduces cost of the tag; and (4) Offer mutual authentication, tag-anonymity and traceability.

The remaining sections of this paper are organized as follows: Section 2 discusses the research background, including communication models, motivation and enabling technologies and its key objectives; Section 3 presents context-aware sensor management systems; Section 4 proposes a novel hash-based RFID mutual authentication protocol; Section 5 presents an informal security and performance analysis; Section 6 demonstrates the experimental analysis using NS-3; and finally Section 7 concludes the research work.

2. System Models

This section discusses the system communication models and research motivation to explain the key factors of hash-based RFID authentication.

2.1. System Communication Model

A basic RFID system consists of three communication entities, namely the receiver (reader), transponder (tag) and a backend database such as a server to store and analyze the data. In general, the RFID tags are attached on physical objects that locate and identify physical things among thousands of objects. Each RFID has a small built-in antenna that attaches a microchip with limited memory space to store the identities of data objects [19]. The RFID reader is basically used as a scanner that interrogates the tag information existing in scanning system environment. A server such as a backend database strategically handles the massive amount of generated data for data processing and storage, offering an influential and necessary processing capability and storage space. Furthermore, it operates the system processor to read, manage, control and store the tag data from the attached tags in the RFID reader as illustrated in Figure 1.

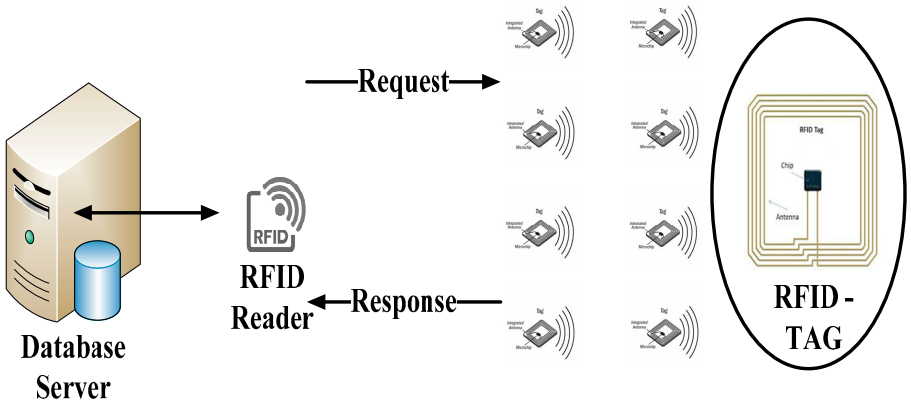

Figure 1. A basic system model of radio frequency identification (RFID).

2.2. Research Motivation

RFID is used to collect the static informational data; however tags cannot extract dynamic informational data, like humidity, acceleration and temperature. On the other hand, sensor systems nowadays are capable to collect all kind of dynamic information data to fill communication gaps using RFID systems. Therefore, the RFID system is integrated with the sensors to collect and monitor the environmental status related to the informational data items. This research refers to a device that integrates a RFID tag and a sensor called Sensing RFID (SRFID). The system device tries to integrate the sensor into an RFID tag to deal with the several challenging issues in large-scale or open-loop systems. The first challenge of the system is the use of non-smart sensors that have specific application requirements for different types of sensors. Moreover, the system models and its related sensor parameters of devices produced by different manufacturers have different types of functionality, even if the sensors are of the same nature.

The following issues are identified, as and when the sensors of the SRFID are configured in a standard way for off-the-shelf readers: (1) SRFID has unique differentiation by the readers; (2) The sensor parameters have automatic sensor recognition features; and (3) The parameters related to the sensor have effective configurations. When the sensor collects the sampling datasets to transfer them to the reader, the datasets, such as parsing and identification, represent additional problems. The identification problems are related to the description of the sensors. The objective of the sensors is to provide interoperability between SRFID tags and readers/host applications, though general purpose sensors, such as analog and digital devices do not have such self-descriptive functions and capability to define the sensors. The second challenge of the system is the data storage related to the SRFID tag. The sensors are diverse in nature, and thus may vary for every SRFID tag. Therefore, the data storage method needs features such as simplicity, flexibility and efficiency. The reader interfaces the various sensors with the application programming interface (API) to access and control all related data of the SRFID tag. Besides, this data storage method allows convenient access to append/remove the sensor from the tag.

The third challenge of the system is the sensor sampling mechanism and it is used to set up an operational mechanism to possess the needed functions to configure, collect and parse the sampling data. To overcome the above challenging problems, this paper focuses on the integral components of an active SRFID tag, namely a self-descriptive sensor, a data storage sensor and an operational sampling sensor. In addition, this paper is restricted to the self-descriptive sensor in consideration of the Plug and Play (PnP) feature [20,21]. In RFID, the issues such as security and privacy are primarily focused on physical [22] as well as security authentication mechanisms [23–25]. As the physical mechanism incurs more additional cost, security authentication schemes are very attractive in practical use. Chien et al. [23], Kim et al. [24,25] and Hajny et al. [12] have studied cross-examination. Since the authentication schemes [12,23–25] do not validate the secret session key of the tag and reader, they are susceptible to various kinds of malicious attacks, such as eavesdropping and tracing, replay, man-in-the-middle and desynchronization. Besides, they do not comply with the security properties of tag anonymity and untraceability.

2.3. Enabling Technologies and Its Key Objectives

The Internet has become more prevalent for social-media networks and various emerging technologies such as wireless sensor networks (WSN), Internet of Things (IoT), cloud computing (CC) and big-data management. These technologies enable people to communicate and share their interests in several ways. As a result, technological advances create new application models and business opportunities to offer comfort, safety, and more computational efficiency. Of late, CC and IoT have been more relevant for industry and academic collaboration. Ashton presented the IoT concept [26] that defines the purpose of physical objects and wireless channels [27]. McCarthy [28] introduced the cloud computing concept that derives a large-scale distributed system to drive several economic benefits such as virtualization, data storage, and computation power.

IoT and CC are service computing platforms that allow object interconnection, including personal and sensitive data, over wireless channels [29–31]. The collective data of physical objects or sensors is generally stored on a cloud-server [32–35]. However, features such as security and privacy are highly demanded to prevent malicious activities [36]. Ferrag et al. [37] and El-Hajj et al. [38] discussed the IoT requirements, including authentication, authorization, confidentiality, privacy and message integrity to signify the importance of node protection. Therefore, to fulfill the standard requirements of an authentication protocol, a suitable mechanism is highly recommended. It can verify the user identities to determine whether he/she is vulnerable or not on open networks [37,38]. Due to network vulnerabilities and Internet security, user authentication plays a crucial role [39].

From the above discussion, the important aspects of RFID authentication protocols have been studied for different IoT environments including industrial management, payment schedules, and several emergency systems. These environments use RFID-tags to achieve more computation power, speed, and physical object robustness than traditional barcode systems. Moreover, technological advancements have addressed several security issues for RFID-based security systems. Concerning the property of untraceability, several RFID-based authentication protocols have simply traded the privacy for the purpose of better system performance. Most of the authentication protocols merely encrypt the tag identity of RFID using cryptographic functions. In case of verification, the reader or back-end server is expected to perform an extensive operation to authorize the RFID-tag, resulting in poor system performance.

Of late, several authentication protocols have been proposed for low-cost RFID systems [40–47]. However, they are reported to have high execution cost, security weaknesses, and vulnerabilities. Chien et al. [40] presented a strong authentication and strong integrity (SASI) protocol that is based on ultra-lightweight authentication. However, their protocol is highly prone to tag tracing and desynchronization attacks [41–43]. To address the critical issues of SASI, Peris-Lopez et al. [44] introduced the Gossamer protocol. Unfortunately, it could not resist desynchronization attacks [45]. Of late, Fan et al. [46] presented an ultra-lightweight authentication for mobile commerce applications including cryptographic operations such as XOR, shift and addition modulo operations, but Aghili and Mala [47] have proven that the Fan et al. scheme cannot resist physical and reader impersonation attacks. Table 1 summarizes the challenging issues of existing RFID-based authentication protocols.

Table 1. Challenging issues of existing RFID-based authentication protocols.

Authentication Protocol	Technique Used	Issue Addressed
Xu et al. [48]	Lightweight Authentication Using Physical Unclonable Function	Susceptible to secret disclosure and desynchronization attack
Bendavid et al. [49]	Lightweight Authentication Using Physical Unclonable Function	Perform frequent execution of setup phase to acquire a new set of pseudo-identity; whereby the back-end server experiences performance deprivation
Gope et al. [50]	Lightweight Anonymous Based Authentication Using Physical Unclonable Function	
Wang et al. [51]	Stability Guaranteed Physical Unclonable Function	
Benssalah et al. [52]	Authentication Using Elliptic Curve Signature with Message Recovery	Incur more communication cost and susceptible to untraceability

To address the above issues, this paper presents a novel hash-based RFID mechanism using synchronized secret session key values. This mechanism tactfully meets the crucial security requirements of IoT-based multimedia systems, namely mutual authentication, untraceability, and resilience to desynchronization attacks. Moreover, it has a built-in context aware management system to handle the storage parameters and thus it can reduce the additional communication cost to improve

the overall system performance. Importantly, it does not perform any exhaustive search to affect the execution of back-end servers.

3. Context-Aware Sensor Management Systems

Figure 2 shows the block diagram of the integration of a virtual TEDS system in IEEE 1451 [53]. The purpose of IEEE 1451 is to identify the parameters of non-smart sensors to access the memory where the datasets related to the TEDS are stored. The IEEE standards, namely IEEE 1451.7 [54], ISO/IEC 24753 [55] and ISO/IEC/IEEE 21451-7 [55] integrate RFID tags and sensors to specify and interface the sensor security and data structure. The standard of ISO/IEC/IEEE 24753.7 is identical to the IEEE standard of 1451.7 which specifies the model related to the application interface to integrate the RFID tag and sensor. This integration is done to execute the functional commands of the sensor application system. These standards integrate the RFID tag and sensor to develop a smart sensor system with RFID tags. However, they do not work with the integral components of existing sensors, such as analog and digital ones to act as a smart sensor system with RFID tags.

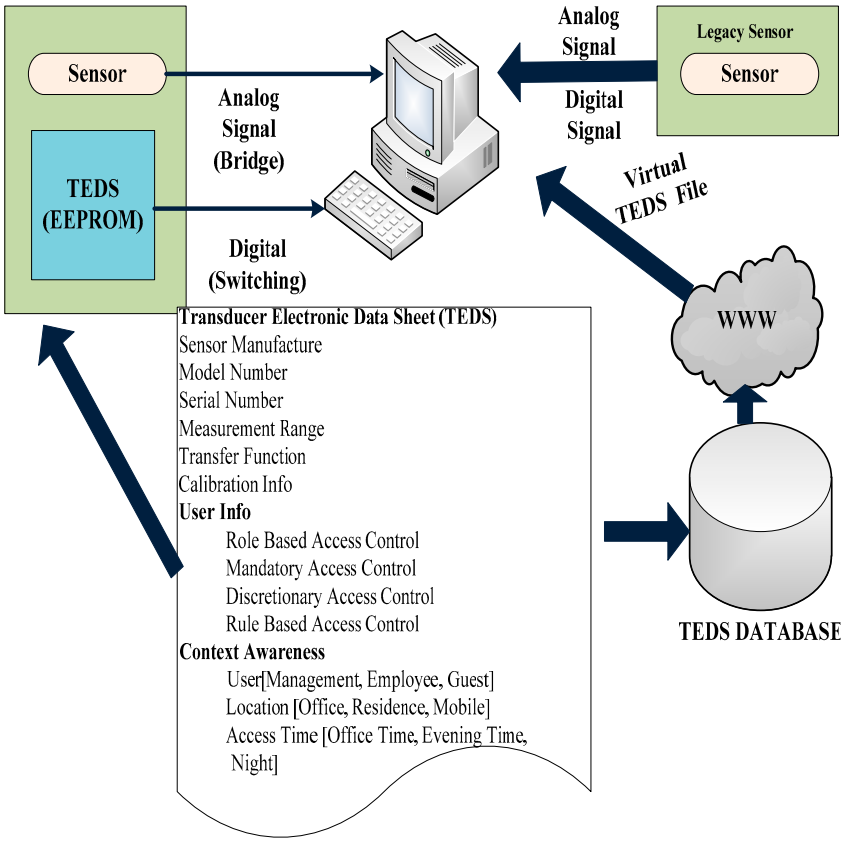

Figure 2. Integration of virtual TEDS systems in IEEE 1451.

The sensor management system has a self-descriptive model like Sensor Web Enablement (SWE) [56–59] initiated by the Open Geospatial Consortium (OGC) to standardize the data encoding and web service interface. In addition, the OGC has built a web-based sensor model for the Sensor Modeling language (SensorML) [21]. The W3C Semantic Sensor Network (SSN) group has proposed an ontology description of SSN [22]. However, these data descriptive sensors are generally employed at the host computer/network level but not the sensor-node level. Moreover, these data descriptive methods use Extensible Markup Language (XML) that has an enormous functional format and thus this language requires an XML-Parser to consume less memory storage.

Therefore, XML files are difficult to deploy in self-descriptive/context-ware sensors to retrieve, remove and modify the sensing data. The self-descriptive/context-aware method is usually not suitable

for sensor application systems, and so this paper proposes a novel strategy to back up the sensing data in the SRFID tags to protect the exchanged information.

4. Novel Hash-Based RFID Mutual Authentication Protocol

A novel hash-based RFID mutual authentication protocol using a secret-session key is proposed. A novel session-key sharing strategy is used to secure the communication between the reader/user and the back-end database server.

Figure 3 illustrates the novel hash-based RFID mechanism. The phases of the mechanism, namely Pre-phase registration, Readers Pro-Tag request and Response, Tag Mutual Session-key Authentication, Back-end Server Key Authentication and Session-key Updating are executed to solve the challenging issues of the existing protocols, such as security, privacy and forgery. To address the issue of security, this paper uses a secret-session key as a significant feature. In addition, the session keys are subsequently generated at the back-end database server $SS_k \rightarrow SS_{k-1}$ to update the output values of the session keys of the tag. Table 2 shows the important notations used in this paper.

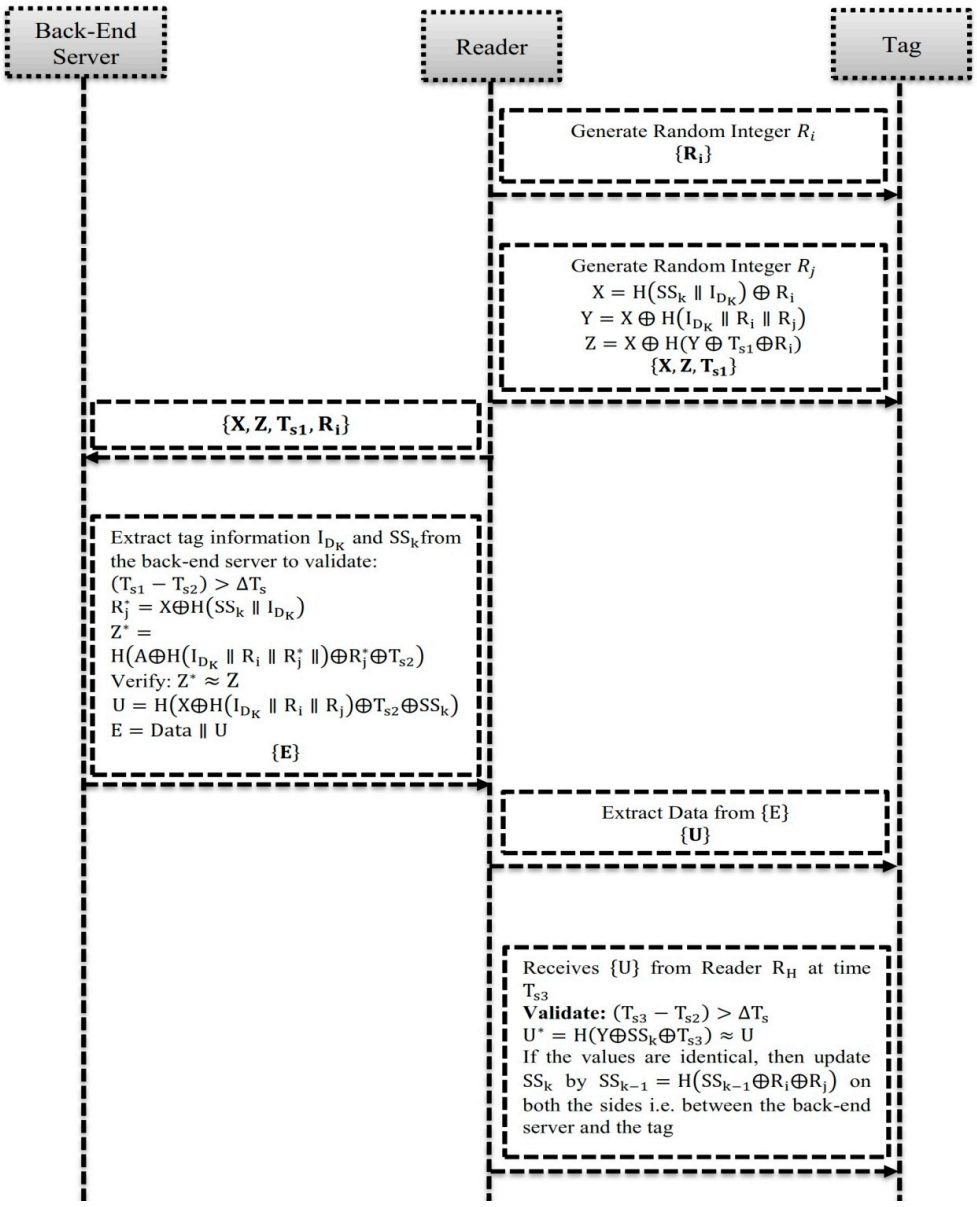

Figure 3. Proposed workflow of the novel hash-based RFID mechanism.

Table 2. Important notations used.

Notation	Description
I_{D_k}	Identity of the k-th Key
I_D	Tag identity
R_i	Random integer generated by reader
R_j	Random integer generated by tag
SS_k	Secret session-key mutually shared between back-end server and tag
SS_{k-1}	Secret session-key in the k-th session
$H(.)$	One-way hash operational function
$\bigoplus$	Bitwise *XOR* operator
ΔT_s	Expected transmission delay
T_{s1}, T_{s2}, T_{s3}	Current timestamps
$\|\|$	Concatenation operator
New_{msg}	Message format

4.1. Phase I: Pre-Phase Registration

The execution flow of the pre-phase registration are as follows:

(1) The back-end database server and the tag mutually share their credentials, such as Tag-I_D : I_{D_K}, one–way hashing, secret – session key : SS_k in the pre-phase registration of the proposed mechanism.
(2) The reader and tag have a unique random number generator to authenticate the services like role assignment. For each tag, the back-end database server collects the parameters, namely I_{D_K}, SS_k, SS_{k-1} and assign the values.
(3) SS_k is the secret-session key of the current session tag k.
(4) SS_{k-1} is the secret-session key of the previous session tag k − 1, since its initial value is set to null.
(5) Data : Information of the object/role that is tagged to the back-end database server to assign the access privileges.

4.2. Phase II: Readers Pro-Tag Request and Response

(1) The reader randomly selects an integer R_i to send a request to the tag.
(2) Then, the tag generates a random integer R_j to compute: $X = H\left(SS_k \,\|\, I_{D_K}\right) \bigoplus R_i$; $Y = X \bigoplus H\left(I_{D_K} \,\|\, R_i \,\|\, R_j\right)$; and $Z = X \bigoplus H\left(Y \bigoplus T_{s1} \bigoplus R_i\right)$, where T_{s1} is the current timestamp of the tag.
(3) After the computation of {X, Y, Z}, the tag sends its response message as {X, Z, T_{s1}} to the reader.
(4) After receiving the response message {X, Z, T_{s1}} from the reader, the reader sends the message of response {X, Z, T_{s1}, R_i} to the back-end server, after being added to the computational integer of R_i.

4.3. Phase III: Tag Mutual Session-Key Authentication

Upon receiving/extracting the tag informational data from the database, the back-end server executes the computational following steps:

(1) If $(T_{s1} - T_{s2}) > \Delta T_s$, then the back-end server terminates the login request of the user, where T_{s2} is the current timestamp in the remote-server and ΔT_s is the expected transmission delay.
(2) Compute: $R_j^* = X \bigoplus H\left(SS_k \,\|\, I_{D_K}\right)$
(3) Validate: $Z^* = H\left(A \bigoplus H\left(I_{D_K} \,\|\, R_i \,\|\, R_j^* \,\|\right) \bigoplus R_j^* \bigoplus T_{s2}\right) \approx Z$
(4) Repeat the execution steps (1) and (5) till the value of Z_i^* is equal to Z_i from the response message of reader. If the values are equaled, then the right tag will be found.
(5) Compute: $U = H\left(X \bigoplus H\left(I_{D_K} \,\|\, R_i \,\|\, R_j\right) \bigoplus T_{s2} \bigoplus SS_k\right)$

Upon receiving the appropriate-tag, the back-end server communicates the tag information to the readers to update the value of secret session-key. In addition to the computation and validation, this phase also executes the following steps to update the readers' session-key:

(1) The back-end server forms a new message format as $New_{msg} = \{Data \parallel U\}$, where Data is the information of the tag to be communicated to the reader to ensure the property of mutual authenticity. If the back-end server fails to deduce a valid right tag, then the server deduces that there is an invalid message authentication to terminate the user session. After the execution of new message New_{msg}, the reader executes the following steps to maintain the communication:
(2) The back-end server sends the new message of $New_{msg} = \{Data \parallel U\}$ to the reader.
(3) Upon receiving the new message of New_{msg} from the back-end server, the reader excludes the parameter of Data and sends the parameter of U to the tag to maintain the communication.

4.4. Phase IV: Back-End Server Key Authentication and Session-Key Updation

Based on the message U at T_{s3}, the tag executes the following steps to authenticate the back-end server:

(1) If $(T_{s3} - T_{s2}) > \Delta T_s$, then the tag terminates the login request of the user, where T_{s3} is the current timestamp in the tag and ΔT_s is the expected transmission delay.
(2) Compute: $U^* = H\left(Y \bigoplus SS_k \bigoplus T_{s3}\right) \approx U$, if the condition is valid, then the tag authenticates the back-end server to confirm that the computed hash value is identical to incur the value of U from the reader.

After the authentication of back-end server, the secret session-key SS_k is updated into SS_{k+1} to server the communication between server and tag.

5. Security and Efficiency Analysis

This section focuses its discussion on the security and performance analysis by comparing the security properties and computation cost with other related protocols [12,24,25].

5.1. BAN Logic Analysis

BAN logic [60] analysis is highly preferred to signify the design process that ensures the security structure of authentication protocol when it starts to build [61]. Moreover, it is a standard way to satisfy the security features of any application system [62,63]. In general, the formal analysis model is comprised of four methods: logical procedure, common analysis, model detection and proof of theorem. This paper chooses BAN logic to verify a belief of agreements as a logical structure [64] in order to analyze the security features of proposed hash-based protocol. The proof of verification is classified into four descriptive parts that are as follows:

A) Protocol Explanation

In this part, the information processes and its related transmission parameters are briefly introduced to entail the structure of the systems where T_R represents the RFID tag, R_H represents the reader and B_S represents the back-end server:

(1) $R_H \rightarrow T_R : \{R_i\}$
(2) $T_R \rightarrow R_H : \{X, Z, T_{s1}\}$
(3) $R_H \rightarrow B_S : \{X, Z, T_{s1}, R_i\}$
(4) $B_S \rightarrow R_H : \{E\}$, where $E = Data \parallel U$
(5) $R_H \rightarrow T_R : \{U\}$, where $U = H\left(X \bigoplus H\left(I_{D_k} \parallel R_i \parallel R_j\right) \bigoplus T_{s2} \bigoplus SS_k\right) \approx U^* = H\left(Y \bigoplus SS_k \bigoplus T_{s3}\right)$

B) Initial Assumption

In this part, the important assumptions of proposed hash-based protocol are listed that are defined as follows:

(1) $T_R| \equiv T_R \overset{I_D, I_{D_k}, SS_k}{\Leftrightarrow} B_S$

(2) $T_R| \equiv T_R \overset{X,Y,Z}{\Leftrightarrow} B_S$

(3) $R_H \Rightarrow U, R_H| \equiv \#(U), R_H| \equiv T_R| \equiv B_S \overset{U}{\leftrightarrow} R_H$

(4) $R_H| \equiv R_H \overset{B_S}{\Leftrightarrow}, B_S| \equiv B_S \overset{R_H}{\Leftrightarrow} R_H$

C) Providing Security Features

In this part, three security features are provided to validate user entities and data synchronization. The detailed user entities are as follows:

(a) $B_S| \equiv R_H| \equiv B_S, R_H| \equiv B_S| \equiv R_H$

(b) $T_R| \equiv B_S| \equiv \{I_D, SS_k\}, B_S| \equiv T_R| \equiv B_S$

(c) $T_R\Big| \equiv B_S \overset{New_{msg}, T_{sNew}}{\leftrightarrow} T_R$

D) Proof of Security Process

The process of security proof explains the representation of A ⊢ B, where A is the premise, B is the conclusion and ⊢ is a symbol of meta-linguistic. From the BAN logic, the seeing rule and the (3) protocol explanation is applied to obtain:

$$R_H \lhd \left\{\left\{\left(SS_k \parallel I_{D_K}\right) \bigoplus R_i\right\}_{R_i}, R_i, \{T_s\}_{X,Z}\right\} \vdash B_S \lhd \left\{\left\{\left(SS_k \parallel I_{D_K}\right) \bigoplus R_i\right\}_{R_i}\right\}$$

From the BAN logic, the freshness rule and the (4) protocol explanation are combined to attain:

$$B_S \lhd \left\{\left\{\left(SS_k \parallel I_{D_K}\right)\right\}_H\right\}, B_S\Big| \equiv (R_i) \vdash B_S \#\left(SS_k \parallel I_{D_K}\right)$$

In case of $R_H| \equiv T_R| \equiv B_S \overset{R_i}{\leftrightarrow} R_H$ i.e., from (3) protocol explanation, it can be obtained as:

$$R_H| \equiv T_R| \equiv R_H \tag{1}$$

Similarly, it can be expressed as:

$$B_S| \equiv R_H| \equiv B_S \tag{2}$$

As a result, the first proven goal ⟨a⟩ is achieved from the given Equations (1) and (2). From the BAN logic, the seeing rule, the (2) and the (3) initial assumptions can be obtained as:

$$T_R\Big| \sim \left\{\left\{\left(I_{D_K} \parallel R_i\right) \bigoplus R_i\right\}_X, \left\{X \bigoplus \left(I_{D_K} \parallel R_i \parallel R_j\right)\right\}_Y, \left\{X \bigoplus \left(I_{D_K} \parallel T_{s1} \parallel R_i\right)\right\}_Z\right\}, T_R\Big| \equiv B_S \overset{X,Y,Z}{\leftrightarrow} T_R$$

$$\vdash B_S \lhd \left\{\left\{\left(I_{D_K} \parallel R_i\right) \bigoplus R_i\right\}, \left\{X \bigoplus \left(I_{D_K} \parallel R_i \parallel R_j\right)\right\}, \left\{X \bigoplus \left(I_{D_K} \parallel T_{s1} \parallel R_i\right)\right\}\right\}$$

From the initial assumption (1), it can be obtained as:

$$T_R| \equiv B_S \Longrightarrow \{X, Z\}, B_S| \equiv \#\left(T_S, I_{D_K}\right) \vdash T_R| \equiv B_S| \equiv \left\{T_S, I_{D_K}\right\} \tag{3}$$

Similarly, it can be expressed as:

$$B_S| \equiv T_R| \equiv B_S \tag{4}$$

As a result, the second proven goal ⟨b⟩ is realized from the given Equations (3) and (4). According to the rule of message-meaning and the (2) initial assumption, it can be expressed as:

$$T_R \Big| \equiv B_S \overset{X,Y,Z}{\leftrightarrow} T_R,\ B_S \lhd \left\{ \left\{ New_{msg}, T_{sNew}, R_i \right\}_{X,Z} \right\} \vdash B_S \Big| \equiv T_R \ \sim \left\{ New_{msg}, T_{sNew}, R_i \right\}$$

Therefore, it can be represented as:

$$T_R \Big| \equiv B_S \overset{X,Y,Z}{\leftrightarrow} T_R, B_S \Big| \Longrightarrow \left\{ New_{msg}, T_{sNew}, R_i \right\} \vdash T_R \Big| \equiv B_S \overset{New_{msg}, T_{sNew}}{\leftrightarrow} T_R \tag{5}$$

Similarly, it can be expressed as:

$$B_S \Big| \equiv T_R \overset{New_{msg}, T_{sNew}}{\leftrightarrow} B_S \tag{6}$$

As a result, the third proven goal ⟨c⟩ is realized from the given Equations (5) and (6).

From the above Equations (1) to (6), the security features ⟨a⟩, ⟨b⟩ and ⟨c⟩ have claimed to be successfully verified. This ensures that the proposed hash-based protocol achieves the property of mutual authentication between the tag, the reader and the back-end server. Moreover, it ensures the security of data synchronization for the proposed hash-based protocol.

5.2. Informal Analysis

The proposed novel hash-based RFID mutual authentication protocol claims that it can provide a high-secure authentication against the most of the potential attacks, namely replay, eavesdropping and man-in-the-middle; since the proposed mechanism is based on the hashing operation and secret session-key synchronization:

Mutual Authentication: The proposed novel hash-based RFID mechanism offers bilateral authentication between the communication parties. The back-end server authenticates the tag by the computation of $Z^* = H\left(A \bigoplus H\left(I_{D_K} \parallel R_i \parallel R_j^* \parallel\right) \bigoplus R_j^* \bigoplus T_{s2}\right)$ on the server-side which will be validated with the received response-message Z sent by the reader. Correspondingly, the back-end server validates its authentication by the computation of $U^* = H\left(Y \bigoplus SS_k \bigoplus T_{s3}\right)$ on the tag-side which will be identical with the received message U sent by the reader.

Resilient to Eavesdropping and Tracing: The proposed novel hash-based RFID mechanism is resilient to eavesdropping and tracing. As the proposed mechanism uses the random integers R_i and R_j and user anonymity, the threat of tracing can be prevented, so none of the messages transport the tag information twice owing to the challenge—response mechanism used by the independent session variables R_i and R_j. The proposed mechanism has limited hash H(.) and X-OR $\bigoplus$ operations with random integers and synchronized-secret operation, therefore any threat of eavesdropping can be avoided by concealing the tag information. Hence, the proposed mechanism can successfully pass a one-way authentication step to prevent the threats, such as eavesdropping and tracing.

Resilient to Replay Attacks: The proposed novel hash-based RFID mechanism can be resilient to replay attacks. As the proposed mechanism often uses the random integers R_i and R_j, the authentication request is verified using $U^* = H\left(Y \bigoplus SS_k \bigoplus T_{s3}\right) \approx U$ to validate whether the current timestamp T_{s3} is fresh or not. After the successful validation, the confidential information will be updated within the valid time-frame. Hence, the attackers can't deduce the information shared between the reader and the tag.

Resilient to Man-in-the-Middle Attacks: As the proposed novel hash-based RFID mechanism uses the hashing and X-OR operations $U = H\left(X \bigoplus H\left(I_{D_K} \parallel R_i \parallel R_j\right) \bigoplus T_{s2} \bigoplus SS_k\right)$ for each message transmission, the parameters SS_k, R_i and R_j can't be tampered with to deduce the confidential information of the tag. Hence, the proposed mechanism can be resilient to man-in-the-middle attacks.

Untraceability and Tag-Anonymity: To hide the tag information, each transaction message and update process consists of some internal parameters SS_k, A and I_{D_K} and also uses the random integers R_i and R_j. The server can deduce the identification of the tag after the successful computation of these parameters SS_k, A and I_{D_K} sent by the tag. Hence, the proposed mechanism stops an attacker from tracing the information of the tag as well as the secret session key of the communication system.

Resilient to Desynchronization Attacks: For the successful launch of desynchronization, an attacker must be able to deduce the secret session key using the related parameters SS_k and SS_{k+1}. In the proposed novel hash-based RFID mechanism, an attacker can't infer the updated value of SS_k as it is associated with the validation of $Z^* = H\left(A \bigoplus H\left(I_{D_K} \| R_i \| R_j^* \|\right) \bigoplus R_j^* \bigoplus T_{s2}\right) \approx Z$.

Hence, the proposed mechanism can be resilient to de-synchronization attack. Table 3 compares the security properties of various hash-based RFID protocols in which the proposed hash-based protocol is proven to be well-secured in comparison with the other hash-based RFID protocols [12,24,25]. Besides, the proposed hash-based protocol meets all the security level of context-aware sensor management systems.

Table 3. Security properties of various hash-based RFID protocols.

Security Properties	Kim et al., 2012 [24]	Kim et al., 2013 [25]	Hajny et al. [12]	Proposed Hash-Based Protocol
Mutual Authentication	Not Support	Partial Support	Not Support	Fully Support
Resilient to Eavesdropping Attack	No	No	No	Yes
Resilient to Tracing Attack	No	No	No	Yes
Resilient to Replay Attack	No	No	No	Yes
Resilient to Man-in-the-Middle Attack	No	No	No	Yes
Resilient to De-Synchronization Attack	No	No	No	Yes
Untraceability and Tag-Anonymity	Not Provided	Not Provided	Not Provided	Provided

5.3. Performance Analysis

In this subsection, the proposed hash-based RFID authentication protocol has been cross-verified with other existing authentication protocols [12,24,25]. To find the computation cost of the authentication protocols, a microcontroller family known as MSP430 simulates the SHA-256 with a frequency of 8 MHz [59]. For SHA-256, this simulator executes the hash function T_{hash} with 0.65 ms. From Table 4, it is observed that the proposed hash-based protocol requires 0.44 ms to complete seven hashing functions. However, Kim et al.'s [24,25] method needs 0.45 ms and 0.61 ms and that of Hajny et al. [12] requires 0.57 ms to complete the execution. Eventually, the proposed hash-based protocol consumes less computation cost in comparison with other existing schemes [12,24,25].

Table 4. Comparison cost of computation efficiency.

Authentication Protocol	RFID -Tag	Reader	Server	Execution Time (ms)	Communication Session	
					Forward Channel	Backward Channel
Kim et al. 2012 [24]	2 T_{hash}	1 T_{hash}	4 T_{hash}	0.45	4	3
Kim et al. 2013 [25]	2 T_{hash}	3 T_{hash}	4 T_{hash}	0.61	4	3
Hajny et al. [12]	2 T_{hash}	2 T_{hash}	4 T_{hash}	0.57	7	4
Proposed Hash-Based Protocol	3 T_{hash}	1 T_{hash}	3 T_{hash}	0.44	3	3

Note that Gope et al.'s method [65] requires a computation time of 0.91 ms to execute 14 T_{hash} functions, which is much more expensive than the proposed hash-based protocol. In view of communication phase interaction, i.e., forward and backward channels, the proposed hash-based protocol finishes the authentication mechanism with less interaction in comparison with other existing protocols [12,24,25]. From Table 4, it is observed that the proposed hash-based protocol invokes three

interactive flows between the tags, the reader and the back-end server, whereas Kim et al. [24,25] and Hajny et al. [12] process four and seven flows, respectively. Moreover, the results prove that the proposed hash-based protocol has less communication cost as compared to other existing protocols [12,24,25], improving the system efficiency. As a result, it is claimed that it can be preferably deployed in IoT-based multimedia systems.

6. Experimental Study

A powerful network simulator known as NS-3 [66] is chosen to simulate the discrete events that construct a modern network environment to investigate the communication metrics such as packet delivery ratio, end-to-end delay and throughput rate. Moreover, this tool uses both IP and non-IP to simulate the network models such as LTE-A, LTE, WiMAX etc. Importantly, it is contained in several library tools to support the required simulation functions [67]. It uses Python and C++ to build or construct the program structure. Table 5 summarizes the important parameters of the NS3 simulator.

Table 5. Important parameters in NS3 Simulator.

System Parameter	Values
Operating System	Ubuntu 16.04 LTS
Simulation Time	1800 s
Area of RFID devices	1500×1000 m^2
Availability of Readers	5 Nos.
Availability of Tags	160 Nos.
Transmission Range of a Reader	200 m
Transmission Range of a Tag	20 m
Communication Environment	IEEE 802.11
Speed of Communication device	1 m/s

Ubuntu 16.04 LTS is preferred to construct the simulation program that is executed for 1800 s. The RFID devices are located in rectangular fashion, which equips 20 tags in a row. To realize the communication structure, the simulation has added eight consecutive rows i.e., 160 tags, where the communication distance is set to be 25 m and the distance between the device and the gateway is assumed to be 275 m Moreover, the simulation has five readers, which can randomly mobilize with a constant speed equal to 1 m/s. The transmission range of a reader and a tag is set to be 200 m and 70 m, respectively [68]. The network environment known as IEEE 802.11 is adopted to test the above scenario. The payload is set to be 48 bytes that randomly sends and receives the information for every 4 s. This scenario is tactfully constructed to examine the communication metrics namely packet delivery ratio, end-to-end delay and throughput rate, respectively.

6.1. Packet Delivery (PR) Ratio

By definition, packet delivery ratio is the ratio between the number of packets sent and the number of packets received successfully by the RFID reader. Most importantly, it is crucial to examine the performance of communication networks.

From Figure 4, it is observed that the packet delivery ratio declines when the number of devices starts to increase. Even if the number of tags reaches 100, the proposed hash-based protocol records less transmission delay between the holding reader and the communication tags in comparison with other existing schemes [12,24,25]. In addition, the result reveals the drawbacks of congestion in low-power wireless environments, where the energy is highly needed to send the data packets. Significantly, it is recorded that the energy spent is dramatically increased when there is more distance between the devices. As a result, a significant value is recommended to calculate a threshold limit, whereby the server can abort a long-distance communication to achieve better performance and device lifetime.

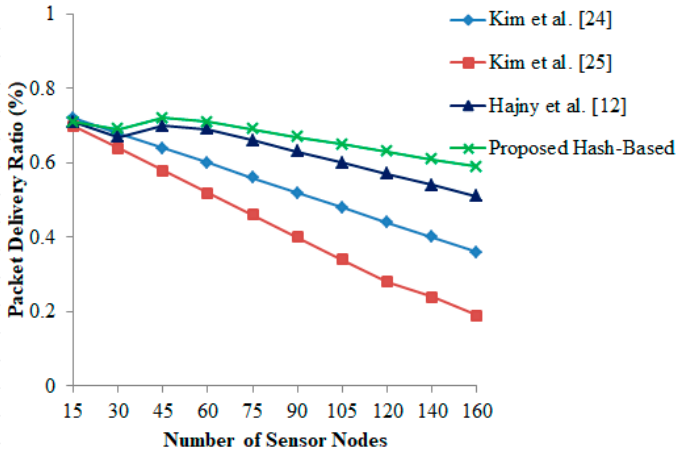

Figure 4. Packet delivery ratio vs. number of sensor nodes.

6.2. End-To-End (E2E) Delay

End-to-end (E2E) delay calculates the average time taken to send and receive the packet between the readers and the tags. It can be defined as the transmission delay, where i is the number of message transmissions, PT_i^r and PT_i^s are the timestamp set for the successful packet sent and received i.e., i-th packet transmission:

$$E2E = \frac{\sum_{i=1}^{N}\left(PT_i^r - PT_i^s\right)}{N} \tag{7}$$

From Figure 5, it is noted that there is a substantial delay when the number of devices starts to increase. Due to repetitive process, more devices are trying to transmit the data packets whereby the high network congestion and distance connectivity is recorded. However, the proposed hash-based scheme has less transmission delay i.e., ~ 0.174 s in comparison with other authentication schemes [12,24,25].

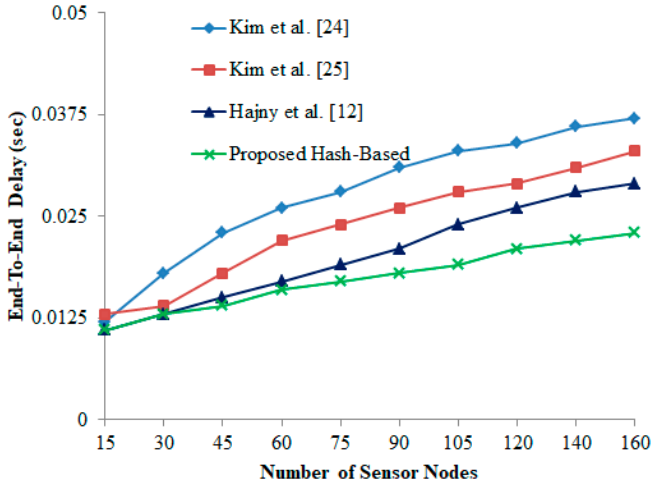

Figure 5. End-to-end delay vs. number of sensor nodes.

6.3. Throughput Rate (TR)

Throughput rate defines the successful transmissions between the server and the reader in ≈ 1 m/s. It can be generally calculated using the following equation, where T_W is the complete execution time, Q_I^R quantity of packet received at the given i-th interval and L_i is the length of transmission i-th interval packet:

$$TR = \frac{\Sigma\left(Q_i^R \times L_i\right)}{T_W} \tag{8}$$

From Figure 6, it is found that the proposed hash-based scheme shows better packet deliverability than other authentication schemes [12,24,25]. It is also evident that the throughput rate naturally declines when the packet deliver ratio is low.

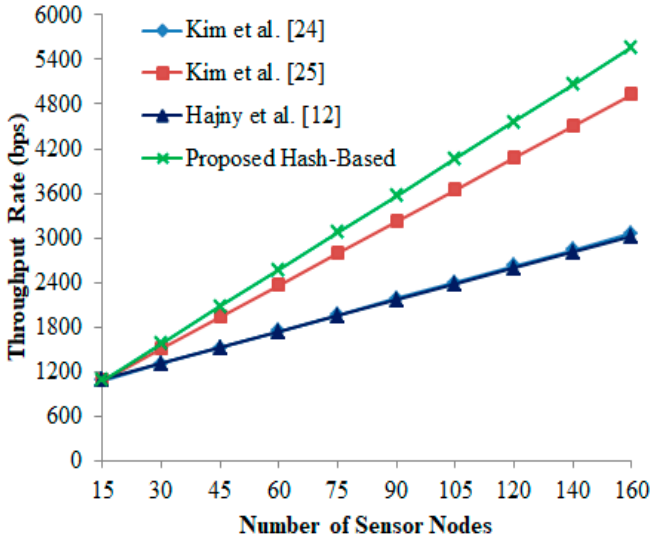

Figure 6. Throughput rate vs. number of sensor nodes.

7. Conclusions

In the past, computing devices have evolved for smart networking that manage sensitive data securely to improve the functioning of the IoT and communication systems. As the device interacts with its own community or infrastructure to collect environmental data over open networks, a secure authentication protocol is highly needed to prevent the unauthorized access. Therefore, a hash-based RFID authentication has been presented as a novel approach for controlling the physical access to devices. It can be useful for the various context-ware sensor management systems. While fixing the device identification and verification, the proposed hash-based RFID mechanism validates the identifier privately using a synchronized secret session key value to strengthen the privacy-enhancement of CASMS. The proposed mechanism uses hashing operations and secret session-key synchronization between the backend server and tag to meet all the security levels of CASMS, namely mutual authentication, untraceability and tag-anonymity. Moreover, the proposed mechanism is resilient to attacks, such as desynchronization, replay and man-in-the-middle. From our informal security and performance analysis, the proposed hash-based protocol achieves better efficiencies than other RFID authentication protocols. Also, the simulation using NS3 shows that the proposed protocol achieves better communication metrics such as packet delivery ratio, end-to-end delay and throughput rate in comparison with other existing schemes [12,24,25]. In the future, an optimized user verification algorithm will be proposed to reduce the operational execution time of the authentication protocol.

Author Contributions: D.B.D. and F.A.-T. have drafted the conceptualization, formal analysis, methodology, investigation and wiring-original draft of this research article. In addition, L.M. has contributed in project administration, resources, data validation and writing–review and editing.

Funding: This research received no external funding.

Acknowledgments: We thank the reviewers and the guest editors for their valuable comments and suggestions.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. El-Hajj, M.; Chamoun, M.; Fadlallah, A.; Serhrouchni, A. Analysis of authentication techniques in Internet of Things (IoT). In Proceedings of the 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, 18–20 October 2017; pp. 1–3.
2. El-hajj, M.; Chamoun, M.; Fadlallah, A.; Serhrouchni, A. Taxonomy of authentication techniques in Internet of Things (IoT). In Proceedings of the 2017 IEEE 15th Student Conference on Research and Development (SCOReD), Putrajaya, Malaysia, 13–14 December 2017; pp. 67–71.
3. Al-Turjman, F.; Malekoo, A. Smart Parking in IoT-enabled Cities: A Survey. *Sustain. Cities Soc.* **2019**, *49*, 101608. [CrossRef]
4. Campioni, F.; Choudhury, S.; Al-Turjman, F. Scheduling RFID Networks in the IoT and Smart Health Era. *J. Ambient Intell. Hum. Comput.* **2019**. [CrossRef]
5. Smartphone Usage Global Stats. Available online: https://www.emarketer.com/Article/Mobile-PhoneSmartphone-Usage-Varies-Globally/1014738 (accessed on 1 April 2018).
6. Xu, W. Mobile applications based on smart wearable devices. In Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems, Seoul, Korea, 1–4 November 2015; pp. 505–506.
7. NIST. Federal information processing standards publication (FIPS 197). In *Advanced Encryption Standard (AES)*; NIST: Gaithersburg, MD, USA, 2001.
8. Vera, S.D.; Bayo, A.; Medrano, N.; Calvo, B.; Celma, S. A Programmable Plug & Play Sensor Interface for WSN Applications. *Sensors* **2011**, *11*, 9009–9032. [PubMed]
9. Hussain, S.A.; Gurkan, D. Management and Plug and Play of Sensor Networks Using SNMP. *IEEE Trans. Instrum. Meas.* **2011**, *60*, 1830–1837. [CrossRef]
10. Spiekermann, S.; Evdokimov, S. Critical RFID privacy-enhancing technologies. *IEEE Secur. Privacy* **2009**, *7*, 56–62. [CrossRef]
11. Higuera, J.; Polo, J.; Gasulla, M. A ZigBee wireless sensor network compliant with the IEEE1451 standard. In Proceedings of the 2009 IEEE Sensors Applications Symposium, New Orleans, LA, USA, 17–19 February 2009.
12. Hajny, J.; Dzurenda, P.; Malina, L. Multidevice Authentication with Strong Privacy Protection. *Wirel. Commun. Mob. Comput.* **2018**. [CrossRef]
13. Song, E.Y.; Lee, K. Understanding IEEE 1451-Networked smart transducer interface standard-What is a smart transducer? *IEEE Instru Meas Mag* **2008**, *11*, 11–17. [CrossRef]
14. *1451.7-IEEE Standard for a Smart Transducer Interface for Sensors and Actuators—Transducers to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet Formats*; IEEE: Piscataway, NJ, USA, 2010; pp. 1–87.
15. ISO/IEC Std FDIS 24753:2010. *Information Technology—Radio Frequency Identification (RFID) for Item Management—Application Protocol: Encoding and Processing Rules for Sensors and Batteries*; ISO: Geneva, Switzerland, 2010; pp. 1–72.
16. Finkenzeller, K. *RFID Handbook*, 2nd ed.; Wiley & Sons: Hoboken, NJ, USA, 2002.
17. EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz–960 MHz Version 1.2.0. Available online: https://www.gs1.org/sites/default/files/docs/epc/uhfc1g2_1_2_0-standard-20080511.pdf (accessed on 12 April 2018).
18. Juels, A. RFID security and privacy: A research survey. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 381–394. [CrossRef]
19. ISO/IEC/IEEE Std 21451-7. *Information Technology—Smart Transducer Interface for Sensors and Actuators—Part 7: Transducer to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats*; ISO: Geneva, Switzerland, 2011; pp. 1–82.
20. Bröring, A.; Echterhoff, J.; Jirka, S.; Simonis, I.; Everding, T.; Stasch, C.; Liang, S.; Lemmens, R. New Generation Sensor Web Enablement. *Sensors* **2011**, *11*, 2652–2699. [CrossRef]
21. Botts, M. *OGC Implementation Specification 07-000: OpenGIS Sensor Model Language (SensorML)*; Open Geospatial Consortium, Inc.: Wayland, MA, USA, 2007; Available online: http://www.opengeospatial.org/standards/sensorml (accessed on 15 July 2014).
22. Compton, M.; Barnaghi, P.; Bermudez, L. The SSN Ontology of the W3C Semantic Sensor Network Incubator Group. *Web Semant.* **2012**, *17*, 25–32. [CrossRef]
23. Chien, H.Y.; Yang, C.C.; Wu, T.C.; Lee, C.F. Two rfid-based solutions to enhance inpatient medication safety. *J. Med. Syst.* **2011**, *35*, 369–375. [CrossRef] [PubMed]

24. Kim, H.S. Enhanced hash-based RFID mutual authentication protocol. *Commun. Comput. Inf. Sci.* **2012**, *339*, 70–77.
25. Kim, H.S. RFID mutual authentication protocol based on synchronized secret. *Int. J. Secur. Appl.* **2013**, *7*, 37–49.
26. Amin, R.; Kumar, N.; Biswas, G.P.; Iqbal, R.; Chang, V. A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment. *Future Gener. Comput. Syst.* **2018**, *78*, 1005–1019. [CrossRef]
27. Noura, M.; Atiquzzman, M.; Gaedke, M. Interoperability in internet of things: Taxonomies and open challenges. *Mob. Netw. Appl.* **2019**, *24*, 796–809. [CrossRef]
28. Foster, I.; Zhao, Y.; Raicu, I.; Lu, S. Cloud computing and grid computing 360-degree compared. In Proceedings of the Workshop on Grid Computing Environments (GCE), Austin, TX, USA, 12–16 November 2008.
29. Fernández Maimó, L.; Huertas Celdrán, A.; Perales Gómez, A.L.; García Clemente, F.J.; Weimer, J.; Lee, I. Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. *Sensors* **2019**, *19*, 1114. [CrossRef] [PubMed]
30. Baker, S.B.; Xiang, W.; Atkinson, I. Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access* **2017**, *5*, 26521–26544. [CrossRef]
31. Jang, Q.; Ma, J.; Yang, C.; Ma, X.; Shen, J.; Chaudhry, S.A. Efficient end-to-end authentication protocol for wearable health monitoring systems. *Comput. Electr. Eng.* **2017**, *63*, 182–195. [CrossRef]
32. Al-Turjman, F.; Abujubbeh, M. IoT-enabled Smart Grid via SM: An Overview. *Future Gener. Comput. Syst.* **2019**, *96*, 579–590. [CrossRef]
33. Perera, C.; Harold Liu, C.; Jayawardena, S.; Chen, M. A survey on internet of things from industrial market perspective. *IEEE Access* **2015**, *2*, 1660–1679. [CrossRef]
34. Al-Turjman, F. *Edge Computing: From Hype to Reality*; Springer: Cham, Switzerland, 2019; ISBN 978-3-319-99060-6.
35. Jiang, Q.; Qian, Y.; Ma, J.; Ma, X.; Cheng, Q.; Wei, F. User centric three-factor authentication protocol for cloud-assited wearable devices. *Int. J. Commun. Syst.* **2009**, *9*, e3900.
36. Alam, M.M.; Malik, H.; Khan, M.I.; Pardy, T.; Kuusik, A.; Le Moullec, Y. A survey on the roles of communication technologies in IoT-based personalized healthcare applications. *IEEE Access* **2018**, *6*, 36611–36631. [CrossRef]
37. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J.; Shu, L. Authentication protocols for internet of things: A comprehensive survey. *Secur. Commun. Netw.* **2017**, *2017*. [CrossRef]
38. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A survey of internet of things (IoT) Authentication schemes. *Sensors* **2019**, *19*, 1141. [CrossRef] [PubMed]
39. Madhusudhan, R.; Mittal, R.C. Dynamic id-based remote user password authentication schemes using smart cards: A review. *J. Netw. Comput. Appl.* **2012**, *35*, 1235–1248. [CrossRef]
40. Chien, H.Y. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. *IEEE Trans. Dependable Secur. Comput.* **2007**, *4*, 337–340. [CrossRef]
41. Cao, T.; Bertino, E.; Lei, H. Security Analysis of the SASI Protocol. *IEEE Trans. Dependable Secur. Comput.* **2009**, *6*, 73–77.
42. Phan, R.C.W. Cryptanalysis of A New Ultralightweight RFID Authentication Protocol—SASI. *IEEE Trans. Dependable Secur. Comput.* **2009**, *6*, 316–320. [CrossRef]
43. Sun, H.M.; Ting, W.C.; Wang, K.H. On the Security of Chien's Ultralightweight RFID Authentication Protocol. *IEEE Trans. Dependable Secur. Comput.* **2011**, *8*, 315–317. [CrossRef]
44. Peris-Lopez, P.; Hernandez-Castro, J.C.; Tapiador, J.M.; Ribagorda, A. Advances in Ultralightweight Cryptography for Low-cost RFID Tags: Gossamer Protocol. In Proceedings of the 9th International Workshop on Information Security Applications, Jeju Island, Korea, 23–25 September 2008; pp. 56–68.
45. Bilal, Z.; Masood, A.; Kausar, F. Security Analysis of Ultra-Lightweight Cryptographic Protocol for Low-cost RFID Tags: Gossamer Protocol. In Proceedings of the 2009 International Conference on Network-Based Information Systems, Indianapolis, IN, USA, 19–21 August 2009; pp. 260–267.
46. Fan, K.; Ge, N.; Gong, Y.; Li, H.; Su, R.; Yang, Y. An Ultra-lightweight RFID Authentication Scheme for Mobile Commerce. *Peer Peer Netw. Appl.* **2017**, *10*, 368–376. [CrossRef]
47. Aghili, S.F.; Mala, H. Security Analysis of an Ultra-lightweight RFID Authentication Protocol for M-commerce. *Int. J. Commun. Syst.* **2019**, *32*, 3837–3852. [CrossRef]
48. Xu, H.; Ding, J.; Li, P.; Zhu, F.; Wang, R. A Lightweight RFID Mutual Authentication Protocol Based on Physical Unclonable Function. *Sensors* **2018**, *18*, 760. [CrossRef] [PubMed]

49. Bendavid, Y.; Bagheri, N.; Safkhani, M.; Rostampour, S. IoT Device Security: Challenging A Lightweight RFID Mutual Authentication Protocol Based on Physical Unclonable Function. *Sensors* **2018**, *18*, 4444. [CrossRef] [PubMed]
50. Gope, P.; Lee, J.; Quek, T.Q. Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2831–2843. [CrossRef]
51. Wang, W.C.; Yona, Y.; Diggavi, S.N.; Gupta, P. Design and Analysis of Stability-guaranteed PUFs. *IEEE Trans. Inf. Forensics Secur.* **2017**, *13*, 978–992. [CrossRef]
52. Benssalah, M.; Djeddou, M.; Drouiche, K. A provably secure RFID authentication protocol based on elliptic curve signature with message recovery suitable for m-Health environments. *Trans Emerg. Telecommun. Technol.* **2017**, *28*, e3166. [CrossRef]
53. Lee, K. IEEE 1451: A standard in support of smart transducer networking. In Proceedings of the 17th IEEE Instrumentation and Measurement Technology Conference [Cat. No. 00CH37066], Baltimore, MD, USA, 1–4 May 2000; pp. 525–528.
54. Zhu, F.; Li, M.; Han, H.; Wang, J. RFIDsense: A reconfigurable RFID sensor tag platform conforming to IEEE 1451.7 standard. In Proceedings of the IEEE 2011 9th IEEE International Conference on ASIC, Xiamen, China, 25–28 October 2011; pp. 1074–1077.
55. Guo, L.; Wu, J.; Xia, Z.; Li, J. Proposed security mechanism for XMPP-based communications of ISO/IEC/IEEE 21451 sensor networks. *IEEE Sens. J* **2014**, *15*, 2577–2586. [CrossRef]
56. Ota, N.; Kramer, W.T. TinyML: Meta-Data for Wireless Networks. Available online: http://www.cs.berkeley.edu/~{}culler/cs294-f03/finalpapers (accessed on 15 July 2014).
57. UPnP Forum. Sensor Management Sensor Data Model Service (Version 1.0). 2013. Available online: http://upnp.org/specs/smgt/ (accessed on 15 July 2014).
58. University of Florida. Sensory Dataset Description Language (SDDL) Specification (Version 1.0). 2009. Available online: http://www.icta.ufl.edu/persim/sddl (accessed on 15 July 2014).
59. Malewski, C.; Simonis, I.; Terhorst, A.; Bröring, A. StarFL—A modularized metadata language for sensor descriptions. *Int. J. Digit. Earth* **2014**, *7*, 450–469. [CrossRef]
60. Burrows, M.; Abadi, M.; Needham, R.M. A logic of authentication. *Proc. R. Soc. Lond. A Math. Phys. Sci.* **1989**, *426*, 233–271. [CrossRef]
61. Fan, K.; Wang, W.; Wang, Y.; Li, H.; Yang, Y. Cloud-Based Lightweight RFID Healthcare Privacy Protection Protocol. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; pp. 1–6.
62. Molnar, D.; Wagner, D. Privacy and security in library RFID: Issues, practices, and architectures. In Proceedings of the 11th ACM Conference on Computer and Communications Security, Washington, DC, USA, 25–29 October 2004; pp. 210–219.
63. Feng, D.G. Research on Theory and Approach of Provable Security. *J. Softw.* **2005**, *16*, 1743–1756. [CrossRef]
64. Syverson, P.F.; Van Oorschot, P.C. On unifying some cryptographic protocol logics. In Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, USA, 16–18 May 1994; pp. 14–28.
65. Gope, P.; Amin, R.; Islam, S.H.; Kumar, N.; Bhalla, V.K. Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *Future Gener. Comput. Syst.* **2018**, *83*, 629–637. [CrossRef]
66. ns3 Network Simulator. Available online: https://www.nsnam.org/ns-3-26/ (accessed on 8 May 2018).
67. Tian, L.; Deronne, S.; Latre, S.; Famaey, J. Implementation and validation of an IEEE 802.11 ah module for ns-3. In Proceedings of the Workshop on ns-3, Seattle, WA, USA, 15–16 June 2016; pp. 49–56.
68. Alghamdi, S.; Schyndel, R.V.; Alahmadi, A. Indoor Navigational Aid Using Active RFID and QR-Code For sighted and Blind People. In Proceedings of the 2013 IEEE Eighth International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Melbourne, VIC, Australia, 2–5 April 2013.