System and Network Security

Open Test (Spring 2021)
International Institute of Information Technology, Hyderabad
Total Marks: 20

Instructions: This is online open test.
Write at the top of your answer book with the following information:
System and Network Security (CS 5470)
Open Test (Spring 2021)
Date: 16-April-2021
Name:
Roll Number:
Hard Deadline: 17-April-2021 (11:55 AM)
Submit your scanned hand-written answer script in the moodle
with the file name: RollNo_OpenTest_16Apr2021.pdf

1. Consider the Rana and Mishra's biometric based content distribution framework for digital rights management systems, which is attached in Appendix-A:

   S. Rana and D. Mishra, "Cryptanalysis and improvement of biometric based content distribution framework for digital rights management systems," *Security and Privacy*. 2021; 4:e133. https://doi.org/10.1002/spy2.133

   With respect to this paper, consider the Rana and Mishra's scheme in Section 4 (pages 7-10). Then, answer the following questions:

   a) Show that their scheme is vulnerable to privileged-insider attack where an insider user of the trusted license server (LS_j) being an attacker can derive the secret credentials of a valid registered user.

   b) Show that their scheme is also insecure against user impersonation attack during the content key acquisition phase.

   [5 + 5 = 10]

2. Consider the scheme in connection with a secure electronic payment system for e-commerce, which is attached in Appendix-B:

   M. A. Hassan, Z. Shukur, and M. K. Hasan, "An Efficient Secure Electronic Payment System for E-Commerce," *Computers*, 2020, 9, 66. https://doi.org/10.3390/computers9030066

   Discuss how this scheme is able to prevent user impersonation attack and also merchant impersonation attack. Explain in detail with appropriate diagrams.

   [5 + 5 = 10]

Appendix-A: S. Rana and D. Mishra, "Cryptanalysis and improvement of biometric based content distribution framework for digital rights management systems," *Security and Privacy*. 2021; 4:e133. https://doi.org/10.1002/spy2.133

Appendix-B: M. A. Hassan, Z. Shukur, and M. K. Hasan, "An Efficient Secure Electronic Payment System for E-Commerce," *Computers*, 2020, 9, 66. https://doi.org/10.3390/computers9030066

********** **End of Question Paper** **********

Received: 6 April 2020 | Revised: 26 July 2020 | Accepted: 5 August 2020 | Published on: 20 October 2020

DOI: 10.1002/spy2.133

RESEARCH ARTICLE

WILEY

Cryptanalysis and improvement of biometric based content distribution framework for digital rights management systems

Saurabh Rana[1] | **Dheerendra Mishra**[2]

[1]Department of Mathematics, The LNM Institute of Information Technology, Jaipur, India

[2]Department of Mathematics, Maulana Azad National Institute of Technology, Bhopal, India

Correspondence
Dheerendra Mishra, Department of Mathematics, Maulana Azad National Institute of Technology, Bhopal 462003, India.
Email: dheerendra.mishrag@lnmiit.ac.in

Abstract

Digital contents are utilized and transmitted over the public network. Thus, the evolution of an emphatic mechanism to ensure authorized access to digital content is the topmost priority of the multimedia industry. Digital right management (DRM) is a tool that aims to ensure authorized access multimedia content to the right holders. However, over the years, several other challenges associated with DRM systems have also emerged such as efficient computation, user privacy, the security of existing protocols. For the scalable distribute digital content, an efficient, secure and authorized content distribution protocol is required. This paper proposed a biometric-based content technique for a DRM system, which enables to deliver content key among mutually authentic entities. The security of the proposed protocol has been proved under the widely recognized random oracle model, which indicates that the proposed protocol is provably secure under probabilistic polynomial time adversary. The proposed scheme achieves anonymity and unlinkability. Moreover, comparative analysis shows that the proposed scheme address efficiency along with security.

KEYWORDS

anonymity, digital rights management systems, key agreement, multimedia, security

1 | INTRODUCTION

A conventional trend of multimedia distribution requires the novel content distribution system for the yield cost of multimedia content. On the other hands, availability of the Internet for common users has presents an efficient platform for digital media distribution, where users do not require to discover a physical space, and it also need not store their content at the physical storage. The content owner now has chosen to adopt a unique way of digital content distribution in which efforts on the production of multiple copied of digital content is no longer required. Digital content can be transmitted or redistributed over the public communication network without actual character degradation and difficulty. It causes rearing piracy, which leads to immense loss to the rights holders in term of revenue.

To protect online content, digital rights management (DRM) systems have been proposed to lead the various application of different areas such as e-commerce, farming theory of law, information theory, and multimedia data protection theory. These systems try to ensure copyright protection by regulating content consumption so that only authorized consumer can access the content. It is one of the widely utilized standards for digital content. In spite of having different

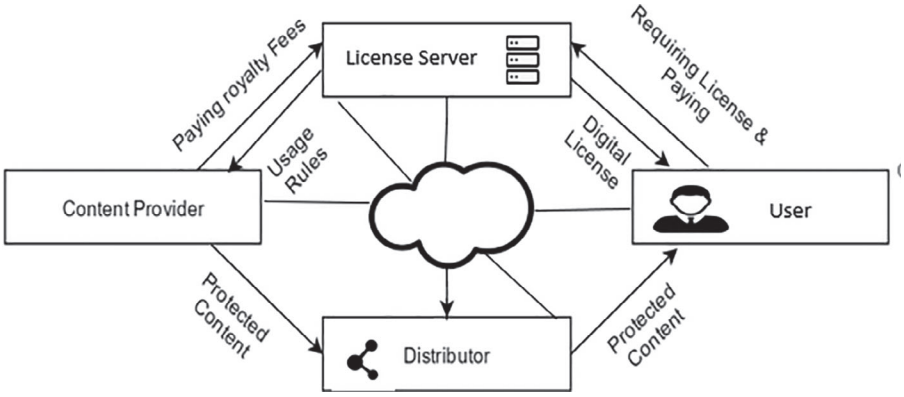

FIGURE 1 Basic digital right management system

DRM implementations, names and ways to facilitate content distribution, the basic architecture is the same as described in Figure 1.

DRM systems present a novel digital content distribution mechanism. This makes distribution much compatible, where any user performs the content play on his connected devices. The license issued by authority may remain valid for a session. Then, the user is not bound to purchase multiple licenses for the same content in order to play on different devices. The trusted authority will analyze and closely monitoring the authorized distribution of digital content.

Accountability has managed through biometric characteristic, which also supports three-factor authentication and gives freedom from long and complex passwords. In 2015, the European Union report accepted a central biometric-based generation system. The biometric-based key production system known as a counter in which biometric characteristic holds the biometrics pattern which previously registered to a service provider with the help user used key.

1.1 | Related work

There are multiple kinds of literature focus on the design of a new DRM system to enhance efficiency and attains security attributes. Initially, Dubl et al[1] introduced the glim of DRM system to understand digital content management. After that many researchers consider DRM system in different contexts.[1-11] But, the most DRM system establishes only unilateral authentication that means the only content provider have an access to check the authenticity of the legal user. As a result, user cannot ensure that he is connecting with the correct server, so he or she has an only personal belief that he or she is connecting with the right server.

Conardo et al[8] gave an identity based DRM protocol, which has two specific phases, two are play and purchase phase respectively. It contrived to ensure privacy and convenience both which transcend the older system. They focus on as following privacy issues: (a) Server should not be able to find a connection between users and contents. (b) The personal information such as identity, the biometric imprint of a user should be anonymous. (c) To ensure prevention of passive attack over the communication between user and server. Nevertheless,[8] DRM system permits a device for verification of the user's of digital content by the trusted authority. Wang et al[9] introduced a novel digital content protection model, which based on iris biometric technique. Wang et al's designed this model to distinguish the client from an unauthorized user. It uses the public key to authenticate server and user. But, there was some low-flow in their schemes such as it did not achieve the security against key transmission attack. In 2008, Chen et al[11] gave a scheme to obtain a compatible and fair use of digital content. Their scheme supported the portability in DRM protocol. But, there was some flaw's in Chen et al scheme such as it is not preventing against session key attack. Zhang et al[12] proposed a protocol on authentication for a DRM environment in which both communication party should verify each other and establish a session.

Yang et al[13] presented cryptanalysis Zhang et al's scheme and observed that it was not resisting for an insider attack and stolen smart card attack. Along with they gave his scheme and claimed that the proposed scheme withstands with all those attacks, that Zhang et al's was not being fulfilled. Mishra et al[14] mentioned that Yang et al improved scheme are also not resisting for denial of service and password guessing attack, even they did not present an active login phase. Tsai et al[15] gave an authentication scheme for distributed mobile service in cloud computing with privacy awareness. Amin et al[16] mentioned that[15] scheme was not preventing for impersonation, passive attacks. Tsai and Lo[17] proposed an session key management protocol without disclosure of the identity of the client, which facilitates access of system

without revealing his or her identity. Chen et al[18] gave a scheme to provide the digital right for accommodating expectations. We analyzed their system and observed that Chen et al's scheme did not achieve security against man in the middle and denial of service attack. However, there are many challenges exist in the rapid development of a DRM system with a biometric-based mechanism. To overcome the above challenges, we design a novel biometric-based authentication mechanism for a DRM system. Which is much more efficient and fulfill the following major requirements: (a) biometric-based based key recognition; (b) smart card cloning; (c) user-friendly DRM system; and (d) authorization of user and server.

After the analysis of the requirement of DRM systems and the cryptanalysis of DRM based authentication schemes, we proposed a new efficient biometric-based authentication scheme for DRM systems. The proposed scheme has been proved through random oracle model, performance analysis of proposed scheme has been performed and shown the enhancement of scheme. The analysis indicates that the proposed scheme is a user-friendly biometric-based authentication scheme that prevents all the existing attack, which occurs in a previous scheme.

1.2 | Our contributions

The concept of authenticated content distribution is highly impactive; many authentication schemes have been proposed to established authorized and secure communication between content distributor and user. However, the above discussed literature suggests many short coming and requirements.

This paper seeks to eliminate some of the issues in the previously proposed schemes and to ensure anonymous and secure environment for DRM systems. It supports to establish a secure and authorized communication among the content distributor and user. Some of the significant contributions are listed below:

- We have discussed the security analysis and contribution of Chen et al's scheme.[18]
- We proposed a ubiquitous and secure architecture for DRM that designed to address existing security threats in content key distribution.
- Proposed scheme security has been proved under the widely accepted random oracle model.
- Proposed scheme satisfies a higher number of security attributes as compared to related schemes.
- The comparative analysis of the proposed scheme in term of computational and communication costs also demonstrates a significant advantage.

1.3 | Organization

The remaining article road map is as follows: In the next Section 2, we present some preliminaries including some assumption and definitions. Section 3 gives the cryptanalysis of Chen et al's scheme. Section 4 gives the proposed content key distribution framework. Section 5 gives a security proof of scheme in the random oracle model and then Section 6 presents performance evaluation and comparison with the existing scheme, where we discuss the related security and performance. Section 7 gives conclusion.

2 | PRELIMINARIES

In this phase, we will discuss the some basic preliminaries, which we have used through-out the paper. Notations exploited in the paper are described in Table 1.

Public key infrastructure (PKI): In cryptography, PKI used for verification of public keys, public key encryption and certificates distribution. In this article, we demonstrate a fundamental infrastructure of a certificate authority (CA). In public-key encryption, CA provides digital certificates for the users and that digital certificates ensure the authenticity of public parameters such as public key, identity, a biometric imprint of the owner. If the owner wishes to register ourselves to the CA then the user shows his valid identity to the *CA*. Then CA issue a certificate for him. In which certificate CA mention a user name, country name, passport number, biometric, validation period, and so on; we summaries it in Figure 2.

TABLE 1 Description of the notations

Notation	Description
p, q	Two large prime
N	Product of two large prime
E	Public key of LS s.t. $1 < e < \varphi(n)$ and $gcd(e, \varphi(n)) = 1$
D	Private key s.t. $d = e^{-1} mod\ \varphi(n)$
$H(.), h(.)$	Strong secure one way hash function
CK	Content key
$E_k(.)$	Symmetric key encryption with key K
$E_{CK}(.)$	Symmetric key encryption with content key CK
LS_j	License server
U_i	User
D	Distributor
CP	Content provider
MD	Metadata
CD	Content
ID_{U_i}	Identity of ith user
ω	Consumer biometric
Ad	Adversary
r_1, r_2, r_3	Random nonce
T_U, T_L	Time stamp

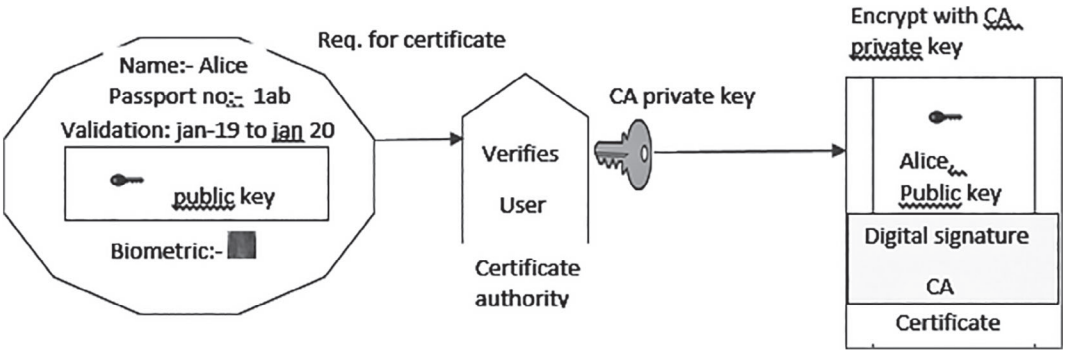

FIGURE 2 Owner certificate

2.1 | Assumption of the authentication scheme for DRM

Assumption 1. There are no known efficient polynomial-time algorithms, which can solve the integer factorization problem.

Assumption 2. The discrete algorithm problem $q^x = p$ where $q, p \in G$ and G be any finite order group. Find x is hard if q, p are given. So we assume that discrete algorithm is hard in existing scheme.

Assumption 3. There are no adversary can encrypt or decrypt E_K, D_K the without knowing the symmetric K.

Assumption 4. Any $h(.)$ should be collision resistance for an arbitrary string x.

2.2 | Adversary model

Under the proposed adversary model, we performs the cryptanalysis in Section 3.

- An adversary is able to eavesdrop all the messages between user and server, which transmits via public channel.
- Any adversary can modify delete and resend all the messages, and can also reroute any message to any other principal.
- An adversary can be a legitimate user or an outsider.
- An adversary have an potential to get some secret credential of user.

3 | CASE STUDY: CHEN ET AL'S DRM SYSTEM

Chen et al's scheme is an authenticated content key distribution mechanism for DRM systems that accommodates user-friendliness attributes of personal use. Their scheme was holding a cleaner balance between user and service providers. Its comparison with related works shows the superiority of their framework. Moreover, it supports portable DRM (P-DRM) systems. As it is a significant result, we discuss its security aspects.

3.1 | Review of Chen et al's protocol for DRM systems

Symbol used in review of Chen et al's scheme[18] is described in Table 1.

3.1.1 | Preliminary distribution for content package phase

CP produces *MD* about *CD* such as identity of content and content provider corresponding, web page URL of LS_j. After that *CP* generates *CK*, encrypts *CD* with E_{CK}, then distributes $\{MD, CK\}$ to LS_j via secure channel, and also upload (MD, E_{CK}) to *D*.

3.1.2 | Registration phase

Any consumer wishes to use the system, he must register himself to LS_j. For this process, U_i should be ready with a unique ID_{U_i} and his ω.

- U_i gives the input as ID_{U_i} and imprint ω. By adopting fuzzy extractor technique, U_i gets uniformly random number R and helper string a and compute $MK_U = h(R\|ID_{U_i}\|a)$. U_i sends $\langle ID_{U_i}, MK_U, a\rangle$ to LS_j.
- LS_j first verifies ID_{U_i}. Then it generates a registration time stamp T_U with the seal of signature (r_U, s_U), where $r_U = {MK_U}^e$ and $s_U = h(ID_{U_i})^d {MK_U}^{H(r_U, a, T_U)}$. LS_j does not store Master key of user. LS_j sends $\langle r_U, s_U, a, T_U\rangle$ to U_i.
- Upon receiving $\langle r_U, s_U, a, T_U\rangle$, U_i first validates a and T_U. U_i wishes to validate signature (r_U, s_U) and checks ${s_U}^e =^? h(ID_{U_i}).r_U^{H(r_U, a, T_U)} modn$. If its holds, then store $\langle r_U, s_U, a, T_U\rangle$.

3.1.3 | License acquisition phase

U_i collects metadata (*MD*) and encrypts content ($E_C K(content)$) from *D*. To recover the encrypted content, U_i buys a valid license.

- U_i gives the input as ID_{U_i} with biometric imprint ω, then fuzzy extractor gives the output (R, a). U_i downloads *MD* and E_{CK} symmetric encryption key, and then uses $\langle r_U, s_U\rangle$ and T_U. U_i sends $\langle MD, ID_{U_i}, r_U, s_U, a, T_U\rangle$ to LS_j via public channel.

- LS_j first verifies T_U and ID_{U_i}. Then, LS_j retrieves the master key $MK_U = {r_U}^d$, where MD is a as an indicator to finding corresponding CK. LS_j compute authentication key $AK_U = h(MK_U, MD, T_L)$, where T_L is the due date of license. LS_j computes $\theta = CK \oplus AK_U$. LS_j puts a signature $S_L = h(\theta, ID_{U_i}, MD, T_L)^d$. LS_j sends $\langle \theta, ID_{U_i}, MD, T_L \rangle$ to U_i.
- Upon receiving $\langle \theta, ID_{U_i}, MD, T_L \rangle$, first U_i validates the license $\mid T'_L - T_L \mid < \Delta T$ by pre-decided threshold value. Then, U_i verifies by the signature ${S_L}^e \stackrel{?}{=} h(\theta, ID_{U_i}, MD, T_L)$. If verification is complete, then U_i easily computes $AK_U = h(MK_U, MD, T_L)$ and $CK = \theta \oplus AK_U$.

3.2 | Cryptanalysis of Chen et al's DRM system

The analysis of the security of Chen et al's scheme[18] is based on the attack model discussed in Section 5.

3.2.1 | Man in middle attack

In general, a man in middle (MIM) is an attack, where the corrupted party secretly interpolates the communication between users and server, who believe that they are directly communicating with each other. When U_i wishes to communicate with the license server the active attack mounts as:

- U_i inputs ID_{U_i} and imprints ω. U_i computes $M_1 = (DID_U \| r_U)^e$ and $V_U = h(DID_U \| K_U \| r_U)$, than sends $\langle MD, ID_{U_i}, r_U, s_U, \alpha, T_U \rangle$.
- Ad intercepts the communication and chooses K for replacing r_U via ${r_U}' = K^e$. Finally, Ad sends $\langle MD, ID_{U_i}, r\prime_U, s_U, \alpha, T_U \rangle$ to LS_j.
- LS_j verifies T_U and ID_{U_i} for correctness of legal user. LS_j computes $MK_U = {r_U}'^d = K$.
- LS_j chooses CK corresponding to MD, and computes $AK_U = h(MK_U, MD, T_L)$, where T_L is a date stamp. LS_j computes $\theta = CK \oplus AK_U$ and $S_L = h(\theta, ID_{U_i}, MD, T_L)^d$. LS_j sends $\langle \theta, S_L, ID_{U_i}, MD, T_L \rangle$.
- Ad again intercepts the communication and gets $\langle \theta, S_L, ID_{U_i}, MD, T_L \rangle$, then executes ${AK_U}' = h(K, MD, T_L)$ using ${AK_U}'$. Finally, Ad retrieves $CK = \theta \oplus {AK_U}'$.

In this attack, even after altering the message, the verification $S_L = h(\theta, ID_{U_i}, MD, T_L)$ succeeds, but the session key and content key is compromised.

3.2.2 | Replay attack

- U_i sends $\langle MD, ID_{U_i}, r_U, s_U, a, T_U \rangle$ to LS_j, where $r_U = {MK_U}^e$, $s_U = h(ID_{U_i})^d {MK_U}^{H(r_U, a, T_U)}$ and T_U is the registration timestamp. LS_j only verifies U_i identity along with registration timestamp.
- Then LS_j executes, the operations to compute the content key for the U_i, and sends the message $\langle \theta, ID_{U_i}, MD, T_L \rangle$ to U_i without verifying the freshness of the content key request, where $S_L = h(\theta, ID_{U_i}, MD, T_L)^d$ and $\theta = CK \oplus AK_U$.
- U_i only verifies the freshness of LS_j generated timestamp and the parameters received from LS_j with the message $\langle \theta, ID_{U_i}, MD, T_L \rangle$ using ${S_L}^e = ?h(\theta, ID_{U_i}, MD, T_L)$, where all the values from the server's newly generated message, so they are valid.

3.2.3 | User impersonation attack

On receiving the user's registration request $\langle ID_{U_i}, MK_U, a \rangle$, LS_j executes the request and provides the login credentials to the user and LS_j does not store user's identity as stated in the registration phase of[18] scheme. Additionally, no mechanism of identity verification is reported. The adversary can use user's identity ID_{U_i} to collect some information to mount the attack as follows:

- Ad selects a value MK_{Ad} and a string a^*, and then sends $< ID_{U_i}, MK_{Ad}, a^* >$ to LS_j.
- LS_j checks ID_{U_i} and generates a registration timestamp T_U^* with the seal of signature (r_U^*, s_U^*), where $r_U^* = (MK_{Ad})^e$, $s_U^* = h(ID_{U_i})^d MK_{Ad}{}^{H(r_U^*, a^*, T_U)}$. LS_j finally sends $\langle r_U^*, s_U^*, a^*, T_U^* \rangle$ to U_i.
- As Ad has MK_{Ad} and a^*, Ad can compute $H(r_U^*, a^*, T_U)$ and $MK_{Ad}{}^{H(r_U^*, a^*, T_U)}$. Now using s_U^* and $MK_{Ad}{}^{H(r_U^*, a^*, T_U)}$, Ad can compute $h(ID_{U_i})^d$.

Due to inefficient registration phase, an Ad can get $h(ID_{U_i})^d$. Now using $h(ID_{U_i})^d$ and $s_U = h(ID_{U_i})^d MK_U{}^{H(r_U, a, T_U)}$, Ad can get U_i's master key as follows:

- Using $h(ID_{U_i})^d$ and s_U, Ad computes $MK_U{}^{H(r_U, a, T_U)}$.
- Ad uses old transmitted message $\langle MD, ID_{U_i}, r_U, s_U, a, T_U \rangle$ to compute $H(r_U, a, T_U)$.
- Using $H(r_U, a, T_U)$ and $MK_U{}^{H(r_U, a, T_U)}$, Ad computes MK_U.

Using old transmitted message $\langle MD, ID_{U_i}, r_U, s_U, a, T_U \rangle$ and MK_U, Ad mounts user impersonation attack as follows:

1. Using old transmitted message $\langle MD, ID_{U_i}, r_U, s_U, a, T_U \rangle$, Ad gets ID_{U_i}, r_U, s_U, a and T_U.
2. For selected MD^*, Ad sends the message $\langle MD^*, ID_{U_i}, r_U, s_U, a, T_U \rangle$ to LS_j.
3. LS_j first verifies T_U and ID_{U_i}, which holds to be valid as used from user communicated message. LS_j retrieves $MK_U = {r_U}^d$. LS_j computes $AK_U^* = h(MK_U, MD^*, T_{L'})$, where $T_{L'}$ is the due date of license. LS_j computes $\theta^* = CK^* \oplus AK_U^*$ and $S_L^* = h(\theta^*, ID_{U_i}, MD^*, T_{L'})^d$. Finally, LS_j sends $\langle \theta^*, ID_{U_i}, MD^*, T_{L'} \rangle$.
4. Using the message $\langle \theta^*, ID_{U_i}, MD^*, T_{L'} \rangle$ and MK_U, Ad can easily extract the content key as follows:
   - Ad computes $AK_U^* = h(MK_U, MD^*, T_{L'})$.
   - Ad computes $CK^* = \theta^* \oplus AK_U^*$, where CK^* is the content key for metadata MD^*.

3.2.4 | No anonymity and unlinkability

During an login phase, U_i sends the message $\langle MD, ID_{U_i}, r_U, s_U, a, T_U \rangle$ to LS_j over the public channel that includes U_i's identity ID_{U_i}. Ad can identify the user and link all the requests. Additionally, Ad can know consumer content selections as login message metadata information. LS_j also response with the message $\langle \theta, ID_{U_i}, MD, T_L \rangle$, which also includes user identity and metadata information. Thus, the adversary can not only know link user communications but also know consumer preferences.

3.2.5 | Inefficient login phase

The login phase of the scheme fails to identify the correctness of login credentials, which may cause denial of service scenario. Even if user inputs incorrect credentials, login phase executes as follows:

- If U_i enters incorrect biometric ω^*. Without verifying the input SC_i sends to the server $\langle MD, ID_{U_i}, r_U, s_U, \alpha, T_U \rangle$.
- LS_j computes $AK_U = h(MK_U, MD, T_L)$ where T_L is a date stamp, $\theta = CK \oplus AK_U$, $S_L = h(\theta, ID_{U_i}, MD, T_L)^d$ and sends $\langle \theta, ID_{U_i}, MD, T_L \rangle$ to U_i.
- U_i can verify ${S_L}^e \neq h(\theta, ID_{U_i}, MD, T_L)$. However, U_i cannot extract content key as correct biometric input is required to compute AK_U.

4 | THE PROPOSED CONTENT DISTRIBUTION FRAMEWORK

To achieve efficient content distribution, we adopt four phases, which notations are defined in Table 1.

1. Content packing.
2. Registration phase.

3. License acquisition phase.
4. Play phase.

4.1 | Content packing

The content provider will adopt following steps for content packing phase.

- Generates the system parameters.
  1. Select two distinct large primes p, q such that $p \neq q$.
  2. Compute $n = p \times q$ where both prime should be have a about half bit length of n. RSA modulo length $\lceil log_2 n \rceil = 1024$ bit, so p, q should be in a 512 bit approx.
  3. Choose $\varphi(n) = (p-1)(q-1)$ value of φ must be kept secret.
  4. Select e such that $1 < e < \varphi(n)$ and $gcd(\varphi(n), e) = 1$.
  5. Compute $d = e^{-1}(mod\varphi(n))$ d also kept secret by respective authority.
  6. Keep (d,e) where d is a private key and e is a public key.
- Compute content key $CK = h(\mathrm{ID}_{DC} \| d \| \mathrm{ID}_{LS})$, where ID_{LS} is the LS identity.
- Encrypt the digital content DC using symmetric key encryption algorithm like AES-256 as $E(DC) = \text{Sym. Enc}_{CK}(DC)$.

4.2 | Registration

To initialize the system, we consider a license server as a trusted authority. This section demonstrates the one-time user registration phase, where the user has to provide his unique identity ID_{U_i} and biometric ω. Using these parameters, the user produces $Gen(\omega)$ with the scanned biological feature ω to extract a uniform randomness R and a helper string, that is, $Gen(\omega) \rightarrow (R, \alpha)$. Finally, U_i sends data on a registration request to a license server. Then, LS_j executes the registration phase of the proposed scheme illustrated in Figure 3. This is explaining in detail as:

Step 1: U_i selects ID_{U_i} and imprints ω. We define a fuzzy extractor $Gen(\cdot)$, which gives the output corresponding to the user imprinted biometric. Then, U_i computes $Gen(\omega) = (R, a)$ and $PWD_U = h(R \| ID_{U_i} \| a)$, and sends $\langle ID_{U_i}, PWD_U \rangle$ to LS via protected channel.

Step 2: After receiving the request form the user side, LS first verifies ID_{U_i}, generates registration time stamp T_U and random number r_1. LS computes $DID_U = (ID_{U_i} \| T_U)^e \bmod n$, $K_U = h(DID_U \| d)$, $Y = K_U \oplus PWD_U$, then finally sends $\langle DID_U, Y \rangle$ to U_i via secure channel.

Step 3: Upon receiving the information, U_i generates first $K_U = PWD_U \oplus Y$. Then, U_i computes $V = h(DID_U \| K_U \| R)$ and finally stores $\langle V, DID_U, Y \rangle$.

User (U)	Secure channel	licence Server (LS_j)
Select ID_{U_i}, imprint ω Generate $Gen(\omega) = (R, a)$ Compute $PWD_U = h(R \| ID_{U_i} \| a)$	$< ID_{U_i}, PWD_U, > \longrightarrow$	Verify ID_{U_i} Generate registration timestamp T_U Generate random value r_1 Compute $DID_U = (ID_{U_i} \| T_R)^e \mod n$ $K_U = h(DID_U \| d)$ $Y = K_U \oplus PWD_U$
$V = h(DID_U \| K_U \| R)$ store $< V, DID_U, Y >$	$\longleftarrow < DID_U, Y >$	

FIGURE 3 Summary of the registration phase

User (U)	Public channel	License server (LS_j)
Input ID_U. Imprint ω. Computes $Gen(\omega) = (R, \alpha)$, Compute $K_U = Y \oplus PWD_U$ Compute $V = h(R\|\|K_U\|\|PWD_U)$ $M_1 = (T_U\|\|DID_U\|\|ID_{DC})^e$ $W_1 = h(K_U\|\|DID_U\|\|T_U)$		
	$< M_1, W_1 >$ $\longrightarrow$	Verifies by ${M_1}^d = (T_U\|\|DID_U\|\|ID_{DC})$ verify $\|T_U - T_U{}'\| < \triangle T$ Compute $K_U = h(DID_U\|\|d)$ Checks $W_1 = ?h(K_U\|\|DID_U\|\|T_U)$ If holds, compute $Z = h(K_U\|\|T_U\|\|W_1)$ $W_2 = h(CK\|\|DID_U\|\|K_U\|\|T_U)$ $S = CK \oplus Z$
	$< W_2, S >$ $\longleftarrow$	
compute $Z = h(W_1\|\|K_U\|\|T_U)$, $CK = S \oplus Z$ check $W_2 = ?h(Ck\|\|DID_U\|\|K_U\|\|T_U)$ if it's holds then Stores CK		

FIGURE 4 Summary of the content key acquisition phase

4.3 | Content key acquisition

If U wants to access digital content on an IoT device. U_i requires SK. To achieve the goal, U demonstrate a content key acquisition phase with S. Once the U_i identity and the imprint is verified, S issues the session key SK, then an illustration of the content key acquisition phase of the proposed scheme shown in Figure 4 and the detailed steps given as.

Step 1: U_i compute $K_U = Y \oplus PWD_U$, with the help of K_U user is able to calculate $V = h(R\|K_U\|PWD_U)$. After this user randomly choose random number r_1 and calculate the value of $M_1 = (T_U\|DID_U\|ID_{DC})^e \ mod \ n$, $W_1 = h(K_U\|DID_U\|T_U)$ and sends $<M_1, W_1, T_U>$ to LS.

Step 2: LS computes first ${M_1}^d = (T_U\|DID_U\|ID_{DU})$, $K_U = h(DID_U\|d)$, and then checks the validation of $W_1 = ?h(K_U\|ID_{U_i}\|d)$. If it holds, then LS processes further and computes $Z = h(K_U\|T_U\|W_1)$, $W_2 = h(CK\|DID_U\|K_U\|r_1)$, $S = CK \oplus Z$, and then sends $<W_2, S>$ to U_i.

Step 3: Upon receiving W_2 and S_j, U_i computes first $Z = h(W_1\|K_U\|T_U)$. With the help of Z, U_i first computes $CK = h(\mathrm{ID}_{DC}\|d\|\mathrm{ID}_{LS})$ and $CK = S \oplus Z$. After the verification of $W_2 = ?h(CK\|ID_{U_i}\|K_U\|T_U)$, U_i stores S_j, if verification hold successfully.

4.4 | Content play

In this section, after a successful login and key acquisition phase, user play content phase and give the input of some parameter for retrieving the session key. If a user is valid, then it will be successful otherwise request is denying. Further process of the phase is the following:

Step 1: U_i physiological imprint $\omega^{'}$ which retrieve from biometric extractor.

Step 2: With the input $\omega^{'}$ and a and reproduce $G_{Rep}(\cdot)$ to retrieve R as $G_{Rep}(\omega^{'}, a) \rightarrow (R)$ if and only if $\omega^{'}$ is very close to ω.

Step 3: U_i obtains content identity ID_{DC}.

Step 4: U_i computes $PWD_U = h(R\|ID_{U_i}\|a)$, then generates $K_U = Y \oplus PWD_U$ verifies $V = ?\, h(R\|K_U\|PWD_U)$.
Step 5: If verification holds, U_i compute (M_1, W_1) respectively. After receiving (M_1, W_1), LS validate the U_i and compute $Z = h(DID_U\|K_U\|ID_{DC})$ and gets $CK = S \oplus Z$.

5 | SECURITY PROOF

Theorem 1. *If The RSA assumption holds then protocol P is CPA secure under random oracle model.*

Proof. We will follow this prove using method of contradiction, so let ∃ probabilistic polynomial time (PPT) adversary A which can break CPA security of proposed protocol, then we construct another PPT adversary B that can break RSA assumptions. That is, if A can break the protocol, then B can break RSA. Thus, ∃ a PPT who have a nonnegligible probability. Then the adversary A invokes simulation queries demonstrated in Figure 5.

- **Game 1:** If A executes a CPA game, then initially Ad have the security parameter 1^n and public key e. Then, Ad do the encryption query q_E for himself. At some point A will send two (M_0, M_1) message form message space. Oracle executes $b \leftarrow 0, 1$ to calculate $C_1 = x^e$ and choose $y \leftarrow 0, 1^n$ to calculate $C_2 = y \oplus m_b$, then finally respond with $c_b = (c_1, c_2)$, which should be cipher text. Eventually, Ad will output $b^{'}$, which is a guess for b. If $b = b'$, then Ad wins the game.
- **Game 2:** If B play a game, which can break the RSA. For a challenger C and we run the $Gen(.)$ algorithm to obtain N, $e, d, x \leftarrow Z_N{*}$. C provides to adversary B $(1^n, e, N, x^e)$, where goal is to return x without having information about d.
- **Game 3:** A really try to achieve y with the following possibility:
- Ad give the random query z to the oracle if $z^e = x^e$ implies $x = z$, then oracle compute $C_1 = x^e$, where $x = DID\|r_1$ calculates $RO(x) = y$ and come up with $y' = y$. It mean that if A has nonnegligible probability of performing such query, then B will have nonnegligible probability. Therefore, B get the advantage to break RSA. But, it is not possible. Thus, B break it with negligible probability. This means A can only have $neg(n)$ probability.
- The second option is that, there is never such a query z such that $z^e = x^e$ so A have no idea about y. Now probability of A win

$$Pr[Awin] = \frac{1}{2}$$

because $C_2 = y \oplus m_b$ behave like a one-time pad with perfect security. But on the other hand A ever manages to query for x or z^e, which is also equal to first step and adversary B is breaking the RSA assumption.

- A wins the game by the step 1 and 2

$$Pr[Awin] = \frac{1}{2} + neg(n)$$

But, we assuming RSA assumption is secure with $neg(n)$ probability. Therefore, proposed scheme is secure.Since we are in the random oracle model (ROM) Ad also has an access to random query, it can be anywhere in the oracle. If Ad send some R' to the random oracle and aspect some y back. ∎

Theorem 2. *Our protocol P has the unconditional user anonymity and intractability property.*

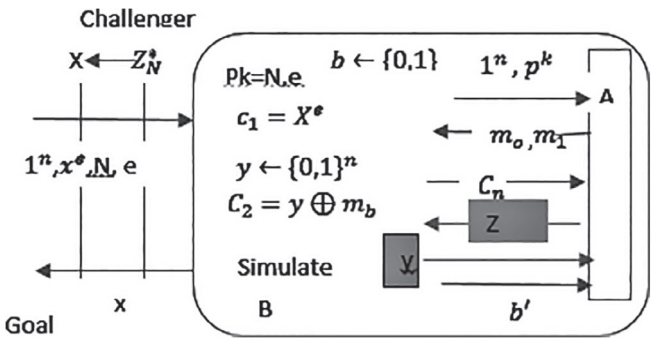

FIGURE 5 Simulation

Proof. Let us suppose random oracle model are CAA secure against PPT *Ad*, which we have proven in Theorem 1 with the help of this result, we to prove user and anonymity and traceability of proposed scheme as following.Of course, fully anonymity implies that we cannot actual sender, we also achieve the traceability.

- Our proposed scheme is unconditional anonymous if the collection of φ_i where $i \in \mathbb{N}$ countably infinite identities. Any random plane text message μ and corresponding cipher text σ cannot be guessed by PPT *Ad* that who actually send the messages with probability better than random guess. So $Ad(A)$ can only give the output to according to real sender with probability $\frac{1}{\varphi_i}$. Since *Ad* play a game, Adversary generate randomly ID_{U_γ} where $\gamma \in (1,2,3, \ldots, i)$ and uniformly distributed $(ID_{U_{\gamma_1}} ID_{U_{\gamma_2}} ID_{U_{\gamma_3}} \ldots ID_{U_{\gamma_i}})$.
- Let us suppose *Ad* guess is correct with the nonnegligible advantage. But still he or she cannot compute $PWD_U = h(R \| ID_{U_i} \| a)$ because for computing PWD_U server user biometrically generated uniformly random number R. So further he or she enable to compute $K_U = Y \oplus PWD_U$. (M_1, W_1) guessing is not possible even *Ad* had non negligible advantage. so *Ad* could not guess which user communicate with the server however distribution $(ID_{U_{\gamma_1}} ID_{U_{\gamma_2}} ID_{U_{\gamma_3}} \ldots \ldots ID_{U_{\gamma_i}}, S)$, So *Ad* could not win the game if advantage will be $\left(\frac{1}{\varphi_i}\right) + neg(n)$. So our satem has unconditional sender anonymity property. ∎

Theorem 3. *In the ROM, if Ad has negligible advantage ε against CAA algorithm, then our protocol P resist against MIM attack*.

Proof. If the *Ad* performs a extraction query q_E in a time t and q_{H_i} query to the oracle H_i. By Theorem 1 ∃ an PPT *Ad* who can solve CAA problem with the advantage.

$$\delta \geq \left(\varepsilon - \frac{1}{2^k}\right)\left(\frac{q_E}{q_H}\right)^{q_E+q_s}\left(\frac{q_H - q_E}{q_H}\right)$$

In this proof, U_i communicate with S_j in a public channel. Which is perform as following.

- U_i give the input as identity ID_{U_i} and biometric ω. Compute $K_U = Y \oplus PWD_U$ and verifies $V = ? h(R \| K_U \| PWD_U)$, if this holds then compute $M_1 = (T_U \| DID_U \| ID_{DC})^e$, $W_1 = h(K_U \| DID_U \| T_U)$ and sends $\langle M_1, W_1 \rangle$ to the S_j via insecure channel.
- If any attacker have the potential to effects communication between U_i and S_j and try to impersinate either M_1 or W_1. So attacker pick any DID_U' randomly and make a time stamp T_U and try to generate a new M_1* but which is not possible because authentication not holds $W_1 \neq h(K_U \| DID_U \| T_U)$ form S_j side.
- Upon receiving $\langle M_1, W_1 \rangle$, the S_j verifies $M_1{}^d = (T_U{}' \| DID_U \| ID_{DC})$ and verifies time stamp, S_j compute $K_U = h(DID_U \| d)$ and checks $W_1 =^? h(K_U \| T_U \| DID_U)$. If verification hold, then compute $Z = h(K_U \| T_U \| W_1)$, $W_2 = h(CK \| ID_{U_i} \| K_U \| T_U)$ and $S = CK \oplus Z$ and sends back $\langle W_2, S \rangle$ to the user via insecure channel.
- If an try attacker impersonate S_j or W_2, attacker not able to generate $Z = h(K_U \| r_1 \| W_1)$. because attacker pick W_1 from insecure channel, but for generating Z he/she must require K_U which is actually protected by DID_U and *LS* private key. So any type impersonation is not possible.
- If any *Ad* pretends to be a U_ith to rip off the digital content form the LS_j, she/he must allow for access the biometric imprint and personal information to register as U_i and After that, it must buy a license for the protected content. So there is no such attacker, who obviously forge a DRM system with some specific credential. In that manner, the protocol P is secure against any *Ad* with MIM.

  Security analysis: Security performance of MIM attack as below.
  - If the attacker attack in an initial phase of the proposed scheme. If any adversary try to guess the correct ID_{U_i} and biometric ω composed with *n* and *m* characters respectively.
  - Then probability of correct guessing of identity and bioimprint $Pr[C_r(ID_{U_i}, \omega)] = \frac{1}{2^{6n+m}}$ approximately.[19] In our scheme private key of *LS* is based on *RSA*, In RSA we assume 2048 bit key size is secure.
  - To retrace *CK* attacker require K_U, for K_U we must know about DID_U and private key of *LS*. For DID_U we must require ID_{U_i} and biometric. So probability of

$$Pr[Ad_{win}] = \frac{1}{2^6 n + m + 2048} \leq neg(n)$$

which is extremely very negligible. After this we can claim that our proposed scheme is secure against any kind impersonation. ■

6 | DISCUSSION ON PERFORMANCE

In this section, we compare our scheme with some other proposed content key distribution schemes that were recently published for DRM architecture as well as some other general key distribution architecture. If the scheme resists attack and fulfills the attribute merit, the symbol ($\surd$) is used. Otherwise, the symbol ($\times$) is used. This security attribute comparison are demonstrated in Table 2.

Furthermore, we demonstrate the efficiency and merit analysis of a given system with a similar type of key distribution systems based on a smart device such as: Wu and Zhou,[21] Tsai and Lo,[17] Xia and Wang,[24] Wang et al scheme,[9] Odelu et al,[23] Wei's et al scheme,[27] Chen et al scheme,[11] Khan et al,[10] and Chen et al.[18]

We considered the symbols as: hash function T_h, T_b bi-linear pairing, T_{me} modular exponentiation, T_{fe}, fuzzy extractor computation, $T_{sym/dec}$ symmetric encryption or decryption, T_{ema} elliptic curve multiplication, T_{ch} chaotic function. We are already aware of the fact that T_h is a very light weight operation as compared to other operations such as T_me, T_fe, and T_b. These can be arranged in the decreasing order of their computational time as: $T_b > T_{ch} > T_{me} > T_{ema} = T_{fe} > T_{sym/dec} > T_h$. The approximate time for computation of the SHA-1 is collected as $T_h \approx 0.00032$ seconds, $T_b \approx 0.380$ seconds, $T_{fe} \approx 0.02102$ seconds, $T_{sym/dec} \approx 0.0056$ seconds, $T_me \approx 0.0192$ seconds, $T_{ch} \approx 0.02102$ seconds and $T_{ema} \approx 0.0171$ seconds is time of an EC scalar multiplication approach respectively.[23,28,29]

In the proposed framework, CK only accessible to the U_ith user, who has purchased a ticket to access the content. However, personal information is public, which is extracting from $Gen(\cdot)$. Then, only U_ith user having his or her unique biometric output trait (R, a) and U_i can retrieve the CK from the LS_j. According to the rule of distribution, only the U_i can give his/her the same digital content to every communication device if he/she transfers the license and personal information by secure channel, such as stores license along with private information in a device memory then transferring by mobile app or Bluetooth technique to the device. Then specific U_i can the transferred or backup data on any device and any time. Indeed, the U_i content portability is well protected.

The CK is protected with the authority generated content Z. It is necessary, U_ith user obtain the random number r_1. Using his secret key d server able to compute Z. At the end LS_j xoring the Z with the CK. Sends to the U_i, so it ensure that U_i secret key is not saved in the data base of LS_j, now, Ad have a only two option to obtain secret key. In the former, the Ad must have to break the integer factoring problem, which we assume to be hard to solve in Assumption 1 and to obtain the LS_j private key d. After that, which is not executable, the Ad require the secret uniformly random output R, which is retrieve form $Gen(\cdot)$ algorithm. However, the uniformly random number R and U_i biometric imprint ω is not transmitted

TABLE 2 Security attributes comparison

Schemes	UA	PG	MIM	SDA	RA	SP
[20]	$\surd$	$\times$	$\surd$	$\times$	$\surd$	$\times$
[21]	$\surd$	$\surd$	$\times$	$\times$	$\surd$	$\times$
[17]	$\surd$	$\surd$	$\surd$	$\times$	$\surd$	$\surd$
[22]	$\surd$	$\surd$	$\surd$	$\times$	$\surd$	$\times$
[23]	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$
[24]	$\surd$	$\surd$	$\surd$	$\times$	$\surd$	$\times$
[25]	$\surd$	$\surd$	$\surd$	$\times$	$\surd$	$\surd$
[11]	$\surd$	$\times$	$\times$	$\times$	$\times$	$\times$
[26]	$\times$	$\surd$	$\times$	$\surd$	$\times$	$\surd$
[18]	$\surd$	$\times$	$\surd$	$\surd$	$\surd$	$\times$
Proposed	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$

Abbreviations: MMA, man-in-the middle attack; PG, off-line password guessing attack; RA, replay attack; SDA, stolen device attack; SP, security proof; UA, user anonymity.

to anyone. The *Ad* not able to use the $Gen(\cdot)$ to extract the uniform randomness in R. Similarly they *Ad* cannot have an idea of output in $Gen(\cdot)$ algorithm. If the *Ad* inputs his/her biometric imprint $\omega^{'}$, then it will be outputted $R' \leftarrow Gen(\omega^{'})$ which is invalid. Because $\omega^{'}$ is not extremely close to ω s.t $|\omega^{'} - \omega| \leq \Delta\omega$ so it does not satisfy his security attributes according to the pre-decided threshold. Hence confidentiality of the *CK* is achieved perfectly.

For computation cost comparison, we compute the performance of proposed scheme from both user and server ends. The total computable operation is $4T_h + 1T_{me} + T_{fe}$ from user side and $4T_h + 1T_{me}$ from server side. Similarly, all remain scheme operations compute in Table 3. After this, user computation cost $4 \times 0.00032 + 1 \times 0.02102 + 1 \times 0.0192$, and computes $4 \times 0.00032 + 1 \times 0.0192$ from server side. In this manner, we compute the all remain scheme performance, which is given in Table 4. The efficiency in term of computation cost are demonstrated in Figure 6.

For the communication cost comparison, we have listed approximate time for the several existing cryptographic operation. We adopt these experimental results from.[30] For comparison, we use RSA modular exponential, which is denoted by T_{me}. In Table 5. To determine the communication overhead of various existing and proposed schemes chooses 128 bit the random nonce, 160 bits for the collision resistance hash function, public encryption scheme RSA for 1024 bits, elliptic curve element consume 320 bits and 32 bits will set for any times stamp. In this paper U_i communicate with LS_j sends $\langle M_1, W_1 \rangle$ where M_1 is an encryption message with PKI. Our protocol defines on 1024 bits RSA system, W_1 is an execution randomly chosen the hash function, which gives the 160 bits output in a his initial transmission. Then, it consumes total number bits $(1024 + 160) = 1184$ bits. After that LS_j respond as $\langle W_2, S \rangle$ so that W_2 has 160 bit and LS_j will take $(160 + 160)$. So total cost will be 1660 bits in both the communication. Then efficiency of the proposed scheme is demonstrated in Figure 7.

TABLE 3 Number of operation required in protocol execution

Schemes/overhead	User side	Service provider side	Trusted party
[20]	$7T_h + 3T_{ch}$	$6T_h + 3T_{ch}$	—
[21]	$T_h + T_b + 3T_{ema} + T_{enc}$	$4T_h + 4T_{ema} + T_{dec}$	$T_{enc} + T_{me}$
[22]	$2T_h + 3T_{ema} + T_b$	$T_b + 3T_{ema} + 2T_h + T_{me}$	—
[17]	$5T_h + T_{me} + T_{ema}$	$5T_h + 3T_{ema} + 2T_b$	—
[23]	$6T_h + T_{me} + 3T_{ema}$	$6T_h + T_{me} + 2T_b + 2T_{ema}$	—
[25]	$2T_{ema} + 3T_h$	$2T_{ema} + 3T_h + T_{me}$	—
[24]	$4T_h + T_{enc}$	$4T_h$	T_{enc}
[11]	$2T_{me} + T_{dec}$	$5T_{me} + T_{sym}$	—
[26]	$3T_{ema} + 4T_h + T_{enc}$	$T_{ema} + 3T_h + T_{dec}$	—
[18]	$2T_h + 1T_{me} + T_{fe}$	$2T_h + 2T_{me}$	—
Proposed	$1T_{me} + 4T_h + T_{fe}$	$1T_{me} + 4T_h$	—

TABLE 4 Total computation time

Schemes	Approx. time (second)
[20]	0.1263
[21]	0.5332
[17]	0.635
[23]	0.5034
[24]	0.0316
[22]	0.984
[25]	0.0896
[11]	0.1456
[26]	0.0969
[18]	0.0885
Proposed	0.0816

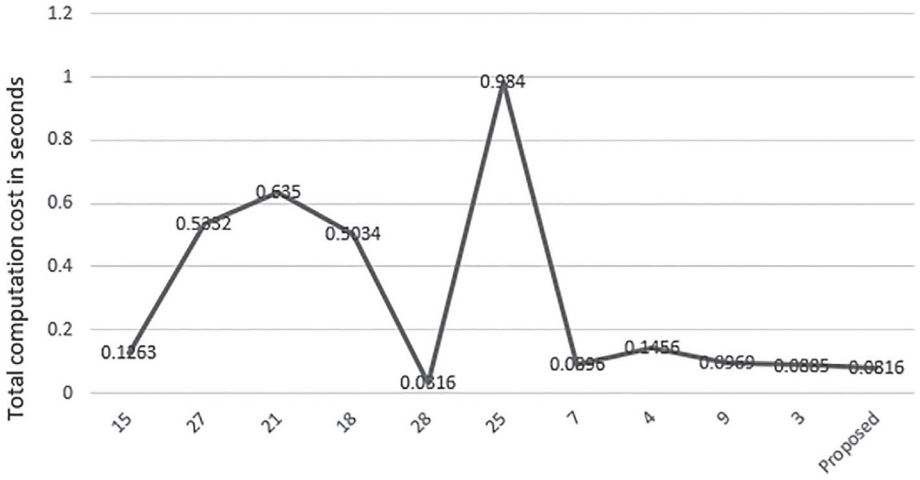

FIGURE 6 Execution cost comparability of the related protocols

TABLE 5 Total communication cost

Schemes	Approx. cost (in bits)	Number of communications
[20]	1320	2
[21]	3648	2
[17]	1408	3
[23]	1920	2
[24]	1376	5
[22]	960	4
[25]	1344	2
[11]	1024	4
[26]	2944	3
[18]	2400	2
Proposed	1660	2

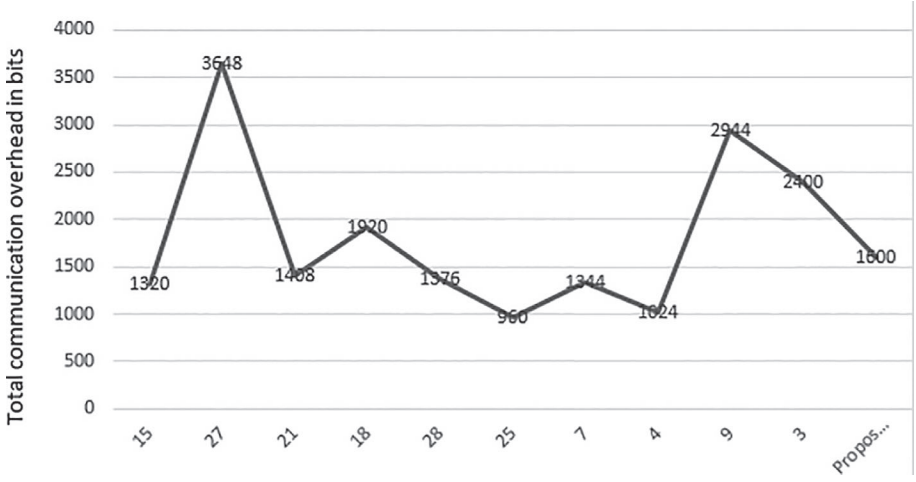

FIGURE 7 Graphical analysis of message overhead

7 | CONCLUSION

A fundamental motivation behind developing DRM systems is always an authorized content distribution. This paper talks about the development of the content distribution mechanism, which indicates the requirement of user-friendly attributes along with security. This paper has introduced an efficient and user-friendly content distribution framework for a DRM system. Each user communicates with mutually authentic content providing authorities anonymously.

Moreover, its security is basically based on PKI infrastructure with unique biometric traits. The security proof of the proposed content distribution framework has been performed under the random oracle model. The analysis of performance is also evaluated. In comparison with the relevant existing schemes, it has identified that the proposed system achieves all the security and performance parameter with validation of proof.

CONFLICT OF INTEREST

All authors declare that they have no conflict of interest.

ORCID

Saurabh Rana https://orcid.org/0000-0003-1583-4510
Dheerendra Mishra https://orcid.org/0000-0001-8115-6397

REFERENCES

1. Duhl J, Kevorkian S. Understanding DRM systems. *An IDC White Paper*; 2001.
2. Vevers R, Hibbert C. Copy protection and content management in the DVB. *IBC Conference Publication, Amsterdam, IBC2002*. IBC Conference Publication, Amsterdam, IBC2002: Citeseer; 2002:458-466.
3. Van Den Heuvel S, Jonker W, Kamperman F, Lenoir P. Secure content management in authorised domains. *Proceedings of IBC*. Citeseer; 2002:467-474.
4. Kwok SH. Digital rights management for the online music business. *ACM Sigecom Exch*. 2002;3(3):17-24.
5. Lee NY, Lee TY. User friendly digital rights management system based on smart cards. *Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09*. New York: IEEE; 2009:869-872.
6. Liu Q, Safavi-Naini R, Sheppard NP. Digital rights management for content distribution. *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003*. Vol 21. Australian Computer Society Inc; 2003:49-58.
7. Michiels S, Verslype K, Joosen W, De Decker B. Towards a software architecture for DRM. *Proceedings of the 5th ACM workshop on Digital rights management*, ACM New York; 2005: 65–74.
8. Conrado C, Kamperman F, Schrijen GJ, Jonker W. Privacy in an identity-based DRM system. *Proceedings. 14th International Workshop on Database and Expert Systems Applications, 2003*. New York: IEEE; 2003:389-395.
9. Wang M, Fan K, Pei Q, Wang S, Cao S. A novel digital content protection system based on iris biometric. *Fourth International Conference on Fuzzy Systems and Knowledge Discovery, 2007. FSKD 2007*. Vol 4. New York: IEEE; 2007:221-225.
10. Khan MK, Kumari S. An authentication scheme for secure access to healthcare services. *J Med Syst*. 2013;37(4):9954.
11. Chen YY, Wang YJ, Chen CJ. A fair-use drm system based on web service. *Eighth International Conference on Intelligent Systems Design and Applications, 2008. ISDA'08*. Vol 3. New York: IEEE; 2008:11-16.
12. Zhang YC, Yang L, Xu P, Zhan YS. A DRM authentication scheme based on smart-card. *International Conference on Computational Intelligence and Security, 2009. CIS'09*. Vol 2. New York: IEEE; 2009:202-207.
13. Yang HW, Yang CC, Lin W. Enhanced digital rights management authentication scheme based on smart card. *IET Information Security*. 2013;7(3):189-194.
14. Mishra D, Mukhopadhyay S. Cryptanalysis of Yang et al.'s digital rights management authentication scheme based on smart card. In: Martínez Pérez G, Thampi SM, Ko R, Shu L. (eds) *Recent Trends in Computer Networks and Distributed Systems Security*. SNDS 2014. Communications in Computer and Information Science. Springer: Berlin, Heidelberg; 2014;420. https://doi.org/10.1007/978-3-642-54525-2_26.
15. Tsai JL, Lo NW. A privacy-aware authentication scheme for distributed mobile cloud computing services. *IEEE Syst. J.* 2015;9(3):805-815.
16. Amin R, Islam SH, Biswas G, Giri D, Khan MK, Kumar N. A more secure and privacy-aware anonymous user authentication scheme for distributed mobile cloud computing environments. *Secur. Commun. Netw.* 2016;9(17):4650-4666.
17. Tsai JL, Lo NW. Secure anonymous key distribution scheme for smart grid. *IEEE Trans. Smart Grid*. 2016;7(2):906-914.
18. Chen HB, Lee WB, Chen TH. A novel DRM scheme for accommodating expectations of personal use. *Multimedia Tools and Applications*. 2018;77(18):23099-23114.
19. Das AK, Goswami A. A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. *J Med Syst*. 2013;37(3):9948.
20. Madhusudhan R, Nayak CS. A robust authentication scheme for telecare medical information systems. *Multimedia Tools and Applications*. 2019;78(11):15255-15273.
21. Wu D, Zhou C. Fault-tolerant and scalable key management for smart grid. *IEEE Trans Smart Grid*. 2011;2(2):375-381.
22. Wang Y. Password protected smart card and memory stick authentication against off-line dictionary attacks. *IFIP International Information Security Conference*. Berlin: Springer; 2012:489-500.
23. Odelu V, Das AK, Wazid M, Conti M. Provably secure authenticated key agreement scheme for smart grid. *IEEE Trans Smart Grid*. 2018;9(3):1900-1910.
24. Xia J, Wang Y. Secure key distribution for the smart grid. *IEEE Trans Smart Grid*. 2012;3(3):1437-1443.
25. Doshi N, Kumari S, Mishra D, Li X, Choo KKR, Sangaiah AK. A password based authentication scheme for wireless multimedia systems. *Multimed Tools Appl*. 2017;76(24):25893-25918.

26. Farash MS, Kumari S, Bakhtiari M. Cryptanalysis and improvement of a robust smart card secured authentication scheme on SIP using elliptic curve cryptography. *Multimed Tools Appl*. 2016;75(8):4485-4504.
27. Wei J, Hu X, Liu W. An improved authentication scheme for telecare medicine information systems. *J Med Syst*. 2012;36(6):3597-3604.
28. Srinivas J, Das AK, Kumar N, Rodrigues JJPC. Cloud centric authentication for wearable healthcare monitoring system. *IEEE Transactions on Dependable and Secure Computing*. 2020;17(5):942-956.
29. Chatterjee S, Roy S, Das AK, Chattopadhyay S, Kumar N, Vasilakos AV. Secure biometric-based authentication scheme using Chebyshev chaotic map for multi-server environment. *IEEE Trans Dependable Secure Comput*. 2018;15(5):824-839.
30. He D, Kumar N, Lee JH, Sherratt RS. Enhanced three-factor security protocol for consumer USB mass storage devices. *IEEE Trans Consumer Electron*. 2014;60(1):30-37.

How to cite this article: Rana S, Mishra D. Cryptanalysis and improvement of biometric based content distribution framework for digital rights management systems. *Security and Privacy*. 2021;4:e133. https://doi.org/10.1002/spy2.133

computers

MDPI

Article

An Efficient Secure Electronic Payment System for E-Commerce

Md Arif Hassan *, Zarina Shukur and Mohammad Kamrul Hasan

Center for Cyber Security, Faculty of Information Science and Technology, National University Malaysia (UKM), UKM, Bangi 43600, Selangor, Malaysia; zarinashukur@ukm.edu.my (Z.S.); mkhasan@ukm.edu.my (M.K.H.)

* Correspondence: arifhassane72@gmail.com; Tel.: +60-102483220

Received: 8 June 2020; Accepted: 22 June 2020; Published: 27 August 2020

Abstract: E-commerce implies an electronic purchasing and marketing process online by using typical Web browsers. As e-commerce is quickly developing on the planet, particularly in recent years, many areas of life are affected, particularly the improvement in how individuals regulate themselves non-financially and financially in different transactions. In electronic payment or e-commerce payment, the gateway is a major component of the structure to assure that such exchanges occur without disputes, while maintaining the common security over such systems. Most Internet payment gateways in e-commerce provide monetary information to customers using trusted third parties directly to a payment gateway. Nonetheless, it is recognized that the cloud Web server is not considered a protected entity. This article aims to develop an efficient and secure electronic payment protocol for e-commerce where consumers can immediately connect with the merchant properly. Interestingly, the proposed system does not require the customer to input his/her identity in the merchant's website even though the customer can hide his/her identity and make a temporary identity to perform the service. It has been found that our protocol has much improved security effectiveness in terms of confidentiality, integrity, non-repudiation, anonymity availability, authentication, and authorization.

Keywords: e-commerce; electronic payments system; payments gateway

1. Introduction

E-commerce was introduced to the consumer and business worlds as a unique approach in 1990 [1]. E-commerce has expanded since then and improved enormously, giving the world's customers and companies incredible benefits. E-commerce history is closely linked to Internet history. When the Internet was open to the public in 1991, online shopping was made possible [1,2]. E-commerce is characterized as a primary business model by means of the selling process of goods, the purchasing of resources, and the distribution or exchange over the Internet of items, services, and knowledge [3]. E-commerce can be used with mobile payment systems, which allows customers to pay for their shopping by using smartphones [4,5]. Mobile business is a major e-commerce extension that enables customers with wireless handheld devices, e.g. tablets, smartphones, and laptops, to carry out online commercial transactions [6]. E-commerce is becoming very popular nowadays since the customer can spend from home; solutions are affordable, with items delivered to the home with no hassle. The popularity of e-commerce is mainly because of its online business perspective. It makes it possible to gain and sell goods online, to provide various services and information through the Internet, and to exchange money immediately between businesses [7]. Many individuals are excited about obtaining their own online website for their company, as it is possible to market items online around the world. Customers are also interested in online shopping since they do not wish to waste valuable time shopping. E-commerce implies an electronic purchasing and marketing process online by using typical Web browsers. It is described as selling and buying of services or goods through wireless technology.

Developed nations tend to be more acquainted with systems, whereas Internet shopping is exploding in developing nations. The foremost goals of an electronic payment system are increasing efficiency, improving protection, and improving customer convenience and ease of use.

In the electronic payment system, the payment gateway is an essential component of the infrastructure to confirm that such exchanges happen with no concerns and to ensure that the common security over electronic systems is maintained [8,9]. Such a system will help secure a purchase along with a person's transaction information. A payment gateway defends transaction information by encrypting personal information, such as credit/debit card details, to guarantee that information is transferred securely between a consumer and the transaction processor. Each online exchange should go through a managed transaction gateway. The secure electronic payment structure includes four system segments [10]. The interaction between the segments operate through protected communication tunnels. Secure communication tunnels offer a protected method for interaction between two or more people, or between segments, such as the buyer to the merchant, on the transaction gateway. The e-payment system must be harmless for online transaction applicants, for instance, fee gateway server, bank account server, and merchant server.

This paper is divided into six sections. Section 1 introduces electronic payments and their related study. Section 2 includes an overview of the existing system and the formulation of the problem. Section 3 describes the RSA cryptosystem. Section 4 addresses how the model will be implemented. Section 5 discusses the security analysis and proposed method advantages. Finally, the last section presents the conclusions and future work.

2. Literature Review

Electronic payment systems have continued to grow over recent years because of the increase of online banking and shopping. As the world advances much more with technological advancements, we are able to see the growth of e-payment methods and transaction processing devices. A payment gateway is a service provider that offers equipment to procedure a transaction between buyers and merchants, along with banks over the World Wide Web. It supports secure a purchase along with a person's transaction information inside a transaction. A payment gateway defends transaction information by encrypting sensitive information, to guarantee the information is transferred securely between a consumer and the transaction processor. To help make it secure between each element, particularly between the client and the Internet payment or merchant gateway, a few strategies are recommended. Specifically, online buyers have to feel comfortable that their personal information and banking details are protected and cannot be seen by hackers. Thus, a connection that is secure it needed to assure payment transactions. Identity theft and phishing fraud are the two most popular types of fraud found within the Internet store [11].

To mitigate both types of fraud, a new secure electronic payment gateway to offer authorization was proposed by Izhar et al. [12]. The main objective of this proposed method was to provide authorization confidentiality, integrity, and availability for transactions. In their study, the authors utilized the Triple Data Encryption Standard (TDES, more often referred to as 3DES) cryptosystem to encrypt the transaction information and accomplish a greater speed of transactions within the payment gateway. The 3DES algorithm utilizes the data encryption standard (DES) cipher three times to encrypt its information. DES is a symmetric key algorithm based on the Feistel cipher [13]. As a symmetric crucial cipher, it applies a similar element for both encryption and decryption processes. The Feistel cipher can make both processes almost precisely the same, which results in an algorithm that is more effective to put into action. DES has both a 64-bit block and key measurement but, in training, grants just 56 bits of security [13]. 3DES was created as a safe option due to DES's small crucial length. In 3DES, the DES algorithm is operated three times with three secrets and is regarded as safe in the event that three individual keys are used. To protect vulnerable cardholder information during transmission, good cryptographic and security protocols must be used. They encourage cryptographic libraries, such as certified AES and 3DES [14]. However, the most recent improvement, referred to as AES, is

slow. Therefore, 3DES is safer and faster [12]. There is another popular cryptosystem used in payment systems [15], namely RSA. An RSA e-commerce security system (RSA-ESS) is implemented in [16], which resolves the security and privacy issues of credit card information in e-commerce transactions. In such systems, RSA is utilized to key the transaction information and realize greater speed in e-commerce transactions. This method is only used for privacy and security of fee information. A study of privacy and security of the e-banking adoption approach can be found in [17], where the authors proved a secure model of trust in an electronic payment system. Figure 1 shows the functional flow of a payment gateway.

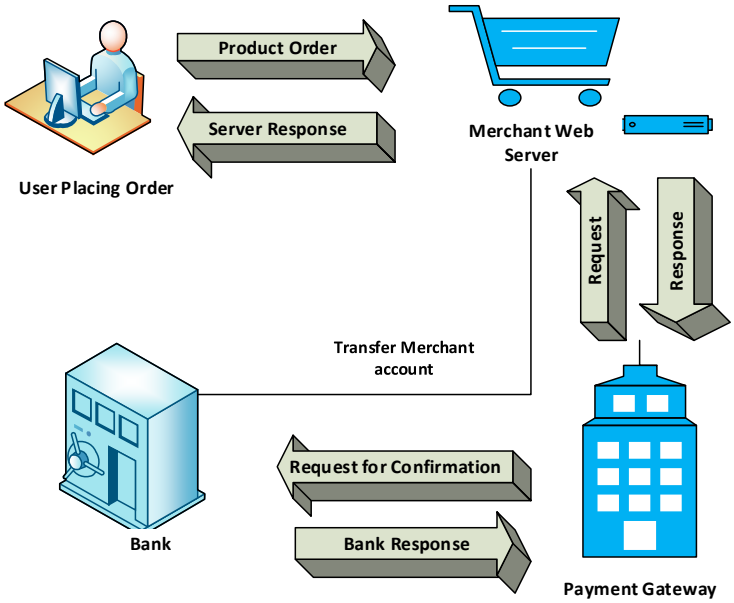

Figure 1. How a payment gateway works [15].

A related review conducted for online banking security and privacy issues in Oman can be found in [18]. A secure and privacy-preserving electronic payment approach can be found in [19], where the authors suggested electronic tokens as being an abstraction of basic fiat currency of equivalent benefit in order to provide privacy and protection in digital payments, presenting an intermediate entity in the method that mediates a transaction between the payer and the payee. A software tool to investigate distributed guessing attacks in the payment transaction process is implemented in [20]. In this study, the authors analyzed that remote Internet banks and merchants with their very own security policies cannot be protected by such attacks. Thus, the number of guessing actions is restricted to avoid repeated invalid efforts produced within a particular time span, and the posting code is confirmed to identify the invalid address information stored by the card-issuing bank account. To obtain credit/debit card details, an adversary is able to utilize a web merchant's transaction page in order to speculate the data: the merchant's reply to some transaction attempt is going to state whether the estimate was correct.

A secure electronic payment gateway for a secure e-payment approach can be found in [21]. In the system, a consumer's monetary information is delivered straight to a transaction gateway, known as a Trusted Third Party (TTP), rather than over an Internet merchant. The method was created by secure socket layer (SSL) with RSA utilized to improve the additional relationship in the payment process. A similar RSA algorithm-based universally unique identifier approach is used to avoid fraudulent activity in e-commerce in [22]. An efficient e-payment protocol for the mobile environment is proposed in [23], where mobile consumers can link directly with the merchant. Presently, numerous techniques are utilized for e-commerce payment systems. In this area, we briefly discuss three existing forms of e-commerce payment. A secure e-commerce protocol is explained here, which is a modified form of an efficient e-electronic for mobile users proposed in [23]. The existing systems and their proposed properties are summarized in Table 1.

Table 1. Related work with their properties.

Author	Method	Remarks	Drawback
Izhar et al. [12]	Triple Data Encryption Standard (TDES)	The proposed system designed and implemented a secure electronic payment gateway to provide authorization, confidentiality, integrity, and availability for transactions.	The proposed method is for the local environment. This payment architecture did not address security issues (i.e., non-repudiation and anonymity).
Nwoye [16]	RSA cryptosystem	The proposed system implemented an RSA e-commerce security system (RSA-ESS), which addresses the security and privacy difficulties with credit card information in e-commerce transactions. In this system, RSA is used to secure payment information and achieve the required speed in an e-commerce transaction.	The proposed system can be used only for the security and privacy of payment information.
Zay Oo [21]	RSA cryptosystem	Through this method, a customer's monetary data (credit or debit card information) are sent straight to a payment gateway, also called TTP, instead of directing them through an online merchant.	The payment gateway plays an essential role as each of the entities communication is concluded in the transaction gateway for the fee payment request. Furthermore, the consumer cannot talk interconnectedly in the merchant to the device doing the payment request. The cardholder and private data are kept in cloud servers and might be subject to compromise of cloud products/services with malware and exploitation of potential vulnerabilities in the program implementation of e-commerce services [24].

3. RSA Cryptosystem

RSA was planned and created by Ron Rivest, Adi Shamir, and Leonard Adleman around 1978 [25]. It is probably the supreme identified cryptosystem for replacing digital or key autograph or perhaps for enciphering chunks of information [26]. The RSA algorithm is the basis of a cryptosystem—a sequence of cryptographic algorithms that are used for special purposes or for specific safety services—that allows public-key encryption and is used extensively for protecting sensitive data, especially if sent via an insecure network such as the Internet [27]. RSA makes use of an adjustable size encryption block along with a variable size key. The RSA algorithm is contingent upon the top number since it is tough to clap the big prime number [28]. It runs on two key numbers to create private and public keys. The sender encodes the idea with the public element of the receiver, and the receiver on buying the idea decrypts it with its own personal key.

RSA usually involves three steps: key generation, decryption, and encryption. RSA has numerous bugs in its strategy and thus is not encouraged for financial use. The most crucial security services that come with RSA are privacy and secrecy, authentication, integrity, and non-repudiation [26], because they prove RSA's being an excellent security public-key cryptosystem. The RSA algorithm has many advantages, namely it has quick encryption and verification processes; offers a high level of security; and sustains data privacy, non-repudiation, and data reliability [22,26,29]. The approach presented in this research paper requires a high level of safety, which can be effectively achieved and

fulfilled by RSA. The following is the algorithm of the RSA cryptosystem. Figure 2 shows how RSA public Key Cryptosystem works [30].

To generate the encryption and decryption keys, we can proceed as follows.

P and Q both Prime, P ≠ Q

∅ = (p-1) (q-1) 1

1 < e <∅

gcd (e,∅) = 1

Public Key = {e, n}

Private Key = {d, n}

Plaintext Encryption:

M < n

Cipher text: C = Me mod n

Cipher text Decryption:

Plaintext: M = Cd mod n

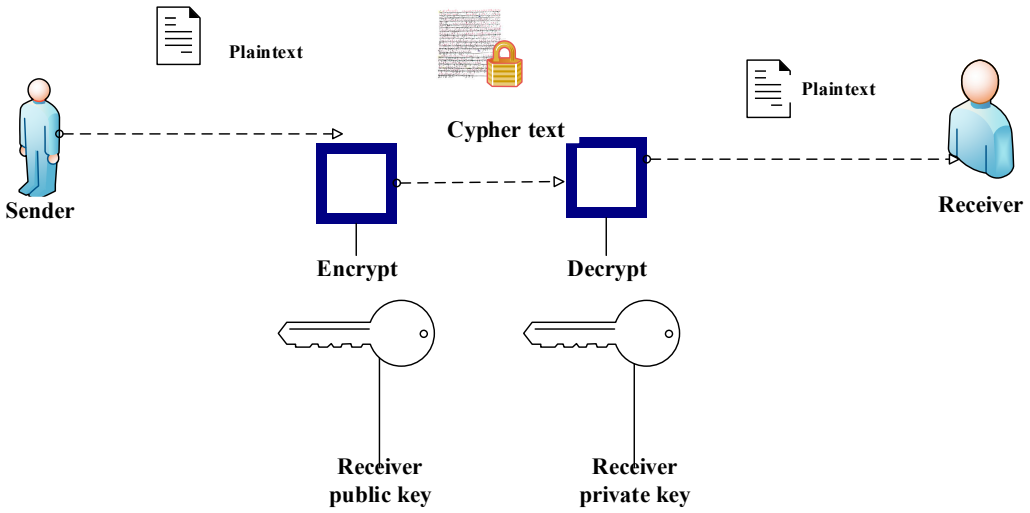

Figure 2. How RSA Public Key Cryptosystem works.

4. The Proposed Method and System Architecture

Security is a key concern and vital issue for the success of e-commerce. In previous work, a secure electronic payment gateway for e-commerce was proposed. In this paper, we propose a secure protocol in e-commerce to enhance the security of the e-commerce process, which can also improve the security of existing work. Interestingly, the proposed system does not require the customer to input his/her identity in the merchant website even though the customer can hide his/her identity and make a temporary identity to process a request for the service. The proposed system is made up of five entities: client (C), merchant (M), payment gateway (PG), user bank (B), and merchant bank.

They perform as follows. Each entity, that is, the client, merchant, user banks, and merchant bank, registers with the payment gateway to create its secret key with the gateway. Secret key elements are necessary to secure communication. Additionally, the user and merchant also create a secret key between themselves. The customer examines the merchant and requests for the product, now with his/her temporary identity created in the merchant website, and the merchant sends the request to the payment gateway. The proposed model of the e-payment system is shown in below Figure 3.

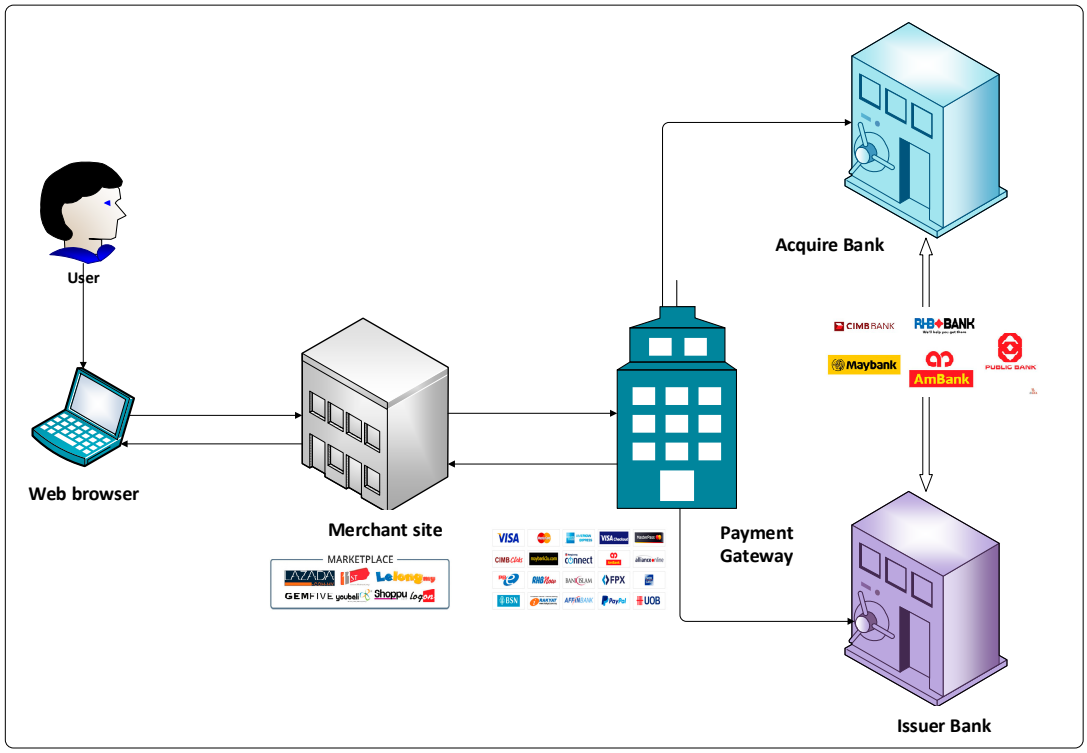

Figure 3. Proposed model of the e-payment system.

The gateway performs several verification steps and forwards the petition to the client's registered bank. At exactly the same time, the payment gateway forwards some encrypted communications to the server. Upon receipt of the quantity subtraction demand, the user bank authenticates it and takes it to the transaction gateway and acknowledges the deduction gateway, after which it sends the authenticated data to the payment gateway. The payment gateway calculates the required result and also forwards it to the bank, wherein the bank captures different versions and amount responses, which are acceptable after verification. The user initiates the transaction by mailing his short-term identity to the server. Be aware that the public key pair continues to be accredited through the certification authority.

4.1. Preliminaries of the Proposed System

- Online customer

A consumer is a person who is going to purchase items by creating payments in a timely manner. In the electronic payment process, an Internet customer is an individual or maybe an organization that gets, consumes, or maybe purchases something online and will choose from various suppliers and goods.

- Merchant

A merchant is an enterprise or a person who offers a service or product. An e-commerce merchant is somebody who offers a service or product solely over the Internet. A merchant sells products to a customer for a price, and, by law, has a duty of hygiene to the consumer because of the expertise of the merchandise he is on the market (e.g., Lazada, Aeon, and Shoppee).

- Client bank

A client bank is a kind of bank that holds the client's account and authorizes him or her during account registration. It generally has the money of numerous customers and is specially designed for the goal of keeping the client's cash on trust (e.g., Maybank, CIMB, and RHB).

- Merchant bank

A merchant bank is a monetary institute, which involves underwriting and company loans, catering mainly to the requirements of big companies and individuals with substantial net worth. In e-commerce, a merchant bank is a kind of bank that permits companies to accept payments through credit or debit cards and is liable for fraud management (i.e., Maybank, CIMB, and RHB).

- Payment gateway

A payment gateway is an essential component of a structure that guarantees worry-free transactions and ensures the common safety among electronic systems. A payment gateway acts as an entrance point to the national banking system [8]. Every transaction that takes place online is created via payment gateways, which serve as points that economic institutions can access. A payment gateway is attached wholly to consumers, banks, and merchants through the Internet and is responsible for the speed, reliability, and safety of all transactions (i.e., ipay88, FPX, and Mol Pay).

4.2. Design Consideration

E-commerce describes all the deals done over the Internet with the help of digital innovation. Mainly, there is an exchange of money for products or solutions across the boundaries of the organization. In this paper, a secure protocol to enhance the security in an e-commerce system is introduced. This secure protocol makes a temporary identity of the client to provide an extra layer of security in e-commerce systems. Whenever the client sends a request to the merchant site for a search of a product, the secure protocol first generates a client's temporary identity to protect client information. Thus, if anything goes wrong during request processing or any malicious data are found, the protocol discards the request and terminates the entire transaction. To understand better, we can classify e-commerce design considerations and challenges separately. From the analysis of the above roles, we can extract some key design considerations for e-commerce.

- Each entity, that is, the client, merchant, user bank, and merchant bank, registers with the payment gateway to create each of their secret key with gateway.
- The client and merchant also create a secret key between themselves.
- The client can connect his/her temporary identity to the merchant site to make an order. After the order has been made, RSA encryption is executed to hide customer card information in order to get ciphertext.
- Once the order has been placed, merchant redirects to the payment gateway for the encryption and decryption processes.
- The client bank along with the client use the RSA signature to execute an electronic signature on the document by making use of the private key.
- The public key set has actually been licensed by a certificate authority.
- The payment gateway executes some verification steps (encryption, decryption, and validation) and forwards value subtraction request to the issuer and some encrypted message to the acquirer. The primary purpose of this system is to create public and private keys for traders and banks. It stores keys in the key database to be distributed to customers after the key generation process. In the decryption process, RSA collects the customer's card details after receipt of the ciphertext from the customers and decrypts the ciphertext. The payment gateway validates the authorization for the payment phase after the customer's card details have been decrypted.
- The ciphertext is decrypted by RSA decryption to get the customer's card information from the bank's website after it receives the ciphertext from the payment gateway. After the customer's card details have been decrypted, the bank shall validate the payment transaction, on the basis of the client's confirmation. Following the transaction, the bank will then inform the customer and the merchant of the payment confirmation.

4.3. Transaction Phase

The customer begins the transaction by mailing his/her momentary identity to the server. In the entire transaction process, the customer immediately contacts the merchant, while, for interaction with the account, the payment gateway was demanded both by the merchant and by the customer to facilitate contact. The symbols used in the transaction phase are as follows:

TIDc—temporary identification of client
IDC—the identity of the product
G—goods details including price, date, and transaction identification
QC ReQ—value claim request
QC ReS—value claim response
PR ReQ—product request
PR ReS—product response
Vs ReQ—value subtraction request
Vs ReS—value subtraction response

A detail explanation of the process is provided below; "Alice' → Bob: C" indicates a message C is delivered to Bob by Alice. The proposed transaction protocol phase is presented in Figure 4.

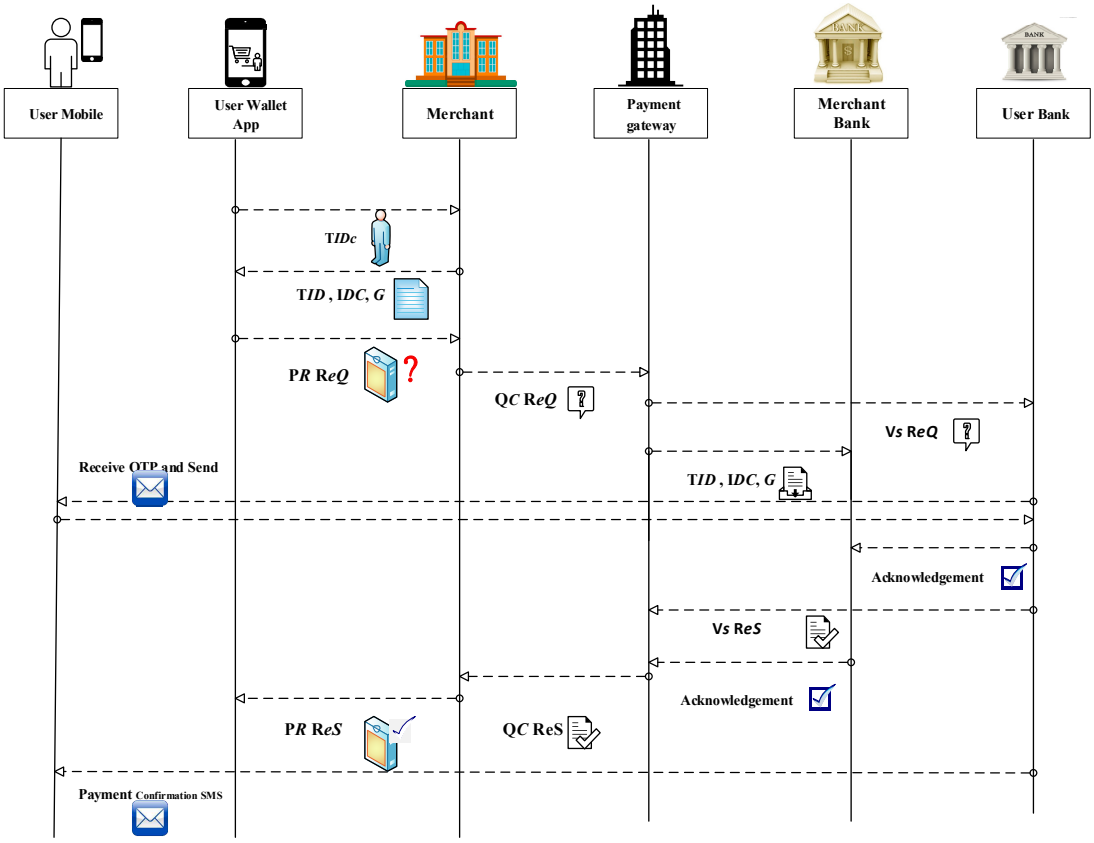

Figure 4. The proposed transaction phase protocol.

Step 1
Start:

Client → Merchant: The client sends a request to the merchant using his/her temporary identity (***TIDc***).

Merchant → Client: The merchant sends back to the client the identity of the product and goods details including price, date, and transaction identification (***IDC, G***).

Step 2

Client → Merchant: The client sends a request for the product (**P*R*** **R*eQ***) to the merchant.

Step 3

Merchant → Payment Gateway: The merchant sends to the payment gateway the value claim request (**Q*C*** **R*eQ***), and the same time payment gateway also (***IDC, G***) to the merchant bank.

Step 4

Payment Gateway → Client Bank: The payment gateway sends the value subtraction request (**V*s*** **R*eQ***) to the client bank.

Step 5

Client Bank → Client Phone: The client bank sends the verification ***OTP*** to the client's mobile phone, and then the client responds to the ***OTP*** verification code. Once verification is complete, the client bank sends an acknowledgment to the merchant bank.

Client Bank → Client: OTP request

Client → Client Bank: OTP response

Merchant → Payment Gateway: Acknowledgment

Step 6

Client Bank → Payment Gateway: The client bank sends the value subtraction response (**V*s*** **R*eS***) to the payment gateway, and the merchant bank sends an acknowledgment to the payment gateway.

Merchant Bank → Payment Gateway: Acknowledgment

Step 7

Payment Gateway → Merchant: The payment gateway sends the value claim response (**Q*C*** **ReS**) to the merchant.

Step 8

Merchant → Client: The merchant sends the product response (**P*R*** **R*eS***) to the client.

Merchant → Client: Acknowledgment

Client Bank → Client: OTP confirmation

Stop:

5. Security Analysis and Advantages

Nowadays, e-commerce is a key component of contemporary businesses. Credit cards or debit cards happen to be popular for remote or on-site transactions, decreasing the demand for inconvenient money transactions. However, along with their popularity comes a substantial number of credit card fraud cases online because of security vulnerability. Solutions have been proposed in the past to avoid the issue, but many of them had been inconvenient and did not satisfy the requirements of merchants and cardholders at exactly the same time. Consumers consider confidentiality, data integrity, authentication, and non-repudiation as essential requirements for creating secure payments over the Web [7,31–34].

- Confidentiality

Confidentiality is important within the e-commerce community because of the chance that hackers might get one's very sensitive information. It is indisputable that, when two parties engage in a transaction, they both usually make sure that it will not be denied. Only an authorized receiver should be able to acquire the encrypted message, so that others cannot read its content [35,36]. In our proposed system, we continually encrypt data before moving it with the additional talking party using the RSA cryptosystem. If opponent A interrupts in between the transaction, it obtains the encrypted note that cannot be decrypted if the key element is missing. Hence, confidentiality is definitely satisfied.

- Integrity

Integrity is one of the major concerns of any company as well as for an e-commerce system. The integrity of the data refers to the concept that information will not be considered a malicious

modification within the system of transmission and that the information is obtained by the receiver at exactly the same time the sender delivered it, that is, the precision of data transmitted to the receiver [37]. The receiver can find out whether any changes were made to the original message. When funds are delivered from customers to suppliers, the integrity of performance should be given particular attention; that is, credit and debit of money must be mapped within an integrated manner.

- Non-repudiation

Non-repudiation signifies that individuals who made a transaction are not able to deny doing it. This means individuals cannot avoid making a payment once electronic signatures are in place. The sender not able to refute he sent a statement. To achieve non-repudiation, plaintext/clear text is used so that people can understand. Ciphertext, which is unreadable to individuals, uses encryption. The reverse procedure is called decryption [36,37]. The issuer makes use of the client's signature to make sure that the legitimate person directs the petition to subtract the payment from his/her bank account. The customer additionally can confirm the issuer's signature. If there are a few issues, the customer along with the issuer cannot deny the fact that they run the signature themselves. Therefore, here non-repudiation is achieved.

- Anonymity

Privacy in e-commerce means anonymity of customers who engage in Internet transactions. The buyer who spends his/her E-cash on something should remain anonymous against the receiver of the cash along with the bank. The possibility for the identity of the buyer to be revealed should happen only when the money is spent illegitimately [38]. Nevertheless, anonymity imposes potential threats, for example counterfeiting, blackmailing, and money laundering. Thus, strengthening anonymity in technologies will ensure the secrecy of the sender's private information and further improve the security of transactions. The examples of personal information that relates to banking are the amount of the transaction and the date and time of the transaction [39]. In our proposed method, the identity of customers is concealed during the transaction, and customers use a short-term identity that is centered on communication. Consequently, it stops the client's anonymity.

- Availability

In e-commerce, services should have accessibility, which not only satisfies the security needs of subjects taking part in a transaction but also provides user comfort. Accessibility is when transactions are done with ease anytime the users wish [40]. Availability describes the accessibility of information resources. In electric payments, availability means prevention against information delays or even removal [41]. The system is liable for delivering, processing, and saving information that will be accessible to those who need it. In our proposed method, every entity is registered with the payment gateway and creates a secret key with the gateway exclusively. Therefore, here availability is achieved.

- Authorization and Authentication

The owners of organizations engaged with financial transactions have implemented different secure authentication and authorization procedures at all stages in order to deter electronic transaction fraud [40]. Only approved users must be eligible on the basis of electronic transfers, and only authorized users must, therefore, be able to access details exchanged for payment [42]. On the other hand, strong client authentication should shield the initiation of online payments besides access [43]. In the proposed method, before the payment procedure, the client bank first asks for client authentication to ensure that the prospect is an authorized person who will receive the verification code to transfer a certain amount from the his/her account to the merchant bank. Therefore, here authorization and authentication are achieved.

Table 2 summarizes the all the security measurements and evaluation that are discussed in Section 5.

Table 2. Security evaluation of the suggested system with related systems.

Parameters	Izhar et al. [12]	Nwoye [16]	Kyaw Zay Oo [21]	Our Proposed Method
Confidentiality	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes
Non-repudiation	No	No	Yes	Yes
Anonymity	No	Yes	No	Yes
Availability	Yes	Yes	Yes	Yes
Authentication	No	No	No	Yes
Authorization	Yes	Yes	Yes	Yes

6. Conclusions

E-commerce has extremely enhanced in popularity over the last decades, and, in methods, it is changing typical payment methods right into online. With the increasing popularity of e-commerce, the market for digital payments has exploded in the last decades, and payment in e-commerce, particularly mobile payment, is currently extremely preferred and plays a growing role. The principal issue is a better requirement for a secure payment system and online authentication on the client side and the Web server side both in growth and in the development of e-commerce. In this research, we suggested an efficient, secure electronic payment system for e-commerce. We introduced a comparison between our suggested framework and the other three existing systems, which use RSA and DES to secure debit/credit card details and keep them anonymous. Most of the clients want an e-commerce program, as there are many advantages. Clients need such a secure system, because it satisfies all specifications and is a sufficient system. We proposed a secure electronic payment system for e-commerce environments on the basis of these requirements. In our proposed method, the transaction gateway functions as a proxy to communicate between the client/merchant and the bank. The security analysis demonstrated that the proposed plan has better protection effectiveness in terms of confidentiality, non-repudiation, integrity, availability, and anonymity. The extension of this article will focus on the utilization of our proposed framework in real-world applications by proving its ability to avoid various attacks and determine the time necessary for electronic payment.

Author Contributions: Conceptualization, M.A.H.; Data curation, M.A.H., Z.S. and M.K.H.; Formal analysis, M.A.H. and Z.S.; Funding acquisition, Z.S. and M.K.H.; Investigation, M.A.H.; Methodology, M.A.H.; Resources, M.A.H.; Software, M.A.H., Z.S., and M.K.H.; Supervision, Z.S. and M.K.H.; Validation, M.A.H. and Z.S.; and Writing—review and editing, M.A.H., Z.S., and M.K.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Malaysia Ministry of Education (FRGS/1/2019/ICT01/UKM/01/2) and Universiti Kebangsaan Malaysia - Yayasan Tun Ismail (EP-2018-012).

Conflicts of Interest: The authors declare no conflict of interest regarding this paper.

References

1. Miva. The History of Ecommerce: How Did It All Begin?—Miva Blog. Available online: https://www.miva.com/blog/the-history-of-ecommerce-how-did-it-all-begin/ (accessed on 16 June 2020).
2. Alam, S.S.; Ali, M.H.; Omar, N.A.; Hussain, W.M.H.W. Customer satisfaction in online shopping in growing markets: An empirical study. *Int. J. Asian Bus. Inf. Manag.* **2020**, *11*, 78–91. [CrossRef]
3. Noor Ardiansah, M.; Chariri, A.; Rahardja, S.; Udin, U. The effect of electronic payments security on e-commerce consumer perception: An extended model of technology acceptance. *Manag. Sci. Lett.* **2020**, *10*, 1473–1480. [CrossRef]
4. Soare, C.A. Internet Banking Two-Factor Authentication using Smartphones. *J. Mob. Embed. Distrib. Syst.* **2012**, *4*, 12–18.

5. Satar, N.S.M.; Dastane, O.; Ma'arif, M.Y. Customer value proposition for E-Commerce: A case study approach. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 454–458. [CrossRef]
6. Narwal, B. Security Analysis and Verification of Authenticated Mobile Payment Protocols. In Proceedings of the 4th International Conference on Information Systems and Computer Networks (ISCON 2019), Mathura, India, 21–22 November 2019; pp. 202–207. [CrossRef]
7. Bezhovski, Z. The Future of the Mobile Payment as Electronic Payment System. *Eur. J. Bus. Manag.* **2016**, *8*, 2222–2839.
8. Masihuddin, M.; Islam Khan, B.U.; Islam Mattoo, M.M.U.; Olanrewaju, R.F. A Survey on E-Payment Systems: Elements, Adoption, Architecture, Challenges and Security Concepts. *Indian J. Sci. Technol.* **2017**, *10*, 1–19. [CrossRef]
9. Liao, X.; Ahmad, K. Factors Affecting Customers Satisfaction on System Quality for E-Commerce. In Proceedings of the 2019 International Conference on Electrical Engineering and Informatics (ICEEI), Bandung, Indonesia, 9–10 July 2019; pp. 360–364. [CrossRef]
10. Mazumder, F.K.; Jahan, I.; Das, U.K. Security in Electronic Payment Transaction. *Int. J. Sci. Eng. Res.* **2015**, *6*, 955–960.
11. Choo, K.K.R. The cyber threat landscape: Challenges and future research directions. *Comput. Secur.* **2011**, *30*, 719–731. [CrossRef]
12. Izhar, A.; Khan, A.; Sikandar, M.; Khiyal, H.; Javed, W.; Baig, S. Designing and Implementation of Electronic Payment Gateway for Developing Countries. *J. Theor. Appl. Inf. Technol.* **2011**, *26*, 3643–3648. [CrossRef]
13. European Union Agency for Cybersecurity. *Algorithms, Key Sizes and Parameters Report—2013*; European Union Agency for Cybersecurity: Eracleon, Greece, 2013; pp. 1–5.
14. Liu, J.; Xiao, Y.; Chen, H.; Ozdemir, S.; Dodle, S.; Singh, V. A survey of payment card industry data security standard. *IEEE Commun. Surv. Tutor.* **2010**, *12*, 287–303. [CrossRef]
15. Pandey, A. Credit Risk Assessment of Payment Gateway Loans for Working Capital Funding of E-Commerce Industry. *Int. Educ. Sci. Res. J.* **2018**, *4*, 2–6. [CrossRef]
16. Nwoye, C.J. Design and Development of an E-Commerce Security Using RSA Cryptosystem. *Int. J. Innov. Res. Inf. Secur.* **2015**, *2*, 2349–7017.
17. Kaur, J.; Singh, H. E-Banking Adoption: A Study of Privacy and Trust. *Int. J. Technol. Comput.* **2017**, *3*, 314–318.
18. Musaev, E.; Yousoof, M. A Review on Internet Banking Security and Privacy Issues in Oman. In Proceedings of the 7th International Conference on Information Technology (ICIT 2015), Chiang Mai, Thailand, 29–30 October 2015; pp. 365–369. [CrossRef]
19. Rajendran, B.; Pandey, A.K.; Bindhumadhava, B.S. Secure and privacy preserving digital payment. In Proceedings of the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), San Francisco, CA, USA, 4–8 August 2017; pp. 1–5. [CrossRef]
20. Ali, M.A.; Arief, B.; Emms, M.; Van Moorsel, A. Does the Online Card Payment Landscape Unwittingly Facilitate Fraud? *IEEE Secur. Priv.* **2017**, *15*, 78–86. [CrossRef]
21. Zay Oo, K. Design and Implementation of Electronic Payment Gateway for Secure Online Payment System. *Int. J. Trend Sci. Res. Dev.* **2019**, *3*, 1329–1334. [CrossRef]
22. Hajira Be, A.B.; Balasubramanian, R. Developing an enhanced high-speed key transmission (EHSKT) technique to avoid fraud activity in E-commerce. *Indones. J. Electr. Eng. Comput. Sci.* **2018**, *12*, 1187–1194. [CrossRef]
23. Mohit, P.; Amin, R.; Biswas, G.P. Design of Secure and Efficient Electronic Payment System for Mobile Users. In *International Conference on Mathematics and Computing*; Springer: Singapore, 2017; Volume 1, pp. 34–43. [CrossRef]
24. European Union Agency for Network and Information Security (ENISA). *Security of Mobile Payments and Digital Wallets*; ENISA: Eracleon, Greece, 2016; ISBN 978-92-9204-199-1.
25. Sharma, M.K. Electronic Cash over the Internet and Security Solutions. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 229.
26. Sharma, N.; Bohra, B. Enhancing Online Banking Authentication using Hybrid Cryptographic method. In Proceedings of the 3rd International Conference on Computational Intelligence and Communication Technology, Ghaziabad, India, 24–26 November 2017; pp. 1–8. [CrossRef]

27. Rouse, M. What is RSA algorithm (Rivest-Shamir-Adleman)?—Definition from WhatIs.com. Available online: https://searchsecurity.techtarget.com/definition/RSA (accessed on 16 June 2020).
28. Balilo, B.B.; Gerardo, B.D.; Byun, Y.; Medina, R.P. Design of physical authentication based on OTP KeyPad. In Proceedings of the 2017 International Conference on Applied Computer and Communication Technologies (ComCom), Jakarta, Indonesia, 17–18 May 2017; pp. 1–5. [CrossRef]
29. Susanna, A.; David, S.; Kathrine, J.W.; Esther, A.G. Enhancing user authentication for mobile wallet using cryptographic algorithm. *J. Adv. Res. Dyn. Control Syst.* **2018**, *10*, 891–897.
30. Sönmez, F.; Abbas, M.K. Development of a Client/Server Cryptography-Based Secure Messaging System Using RSA Algorithm. *J. Manag. Eng. Inf. Technol.* **2017**, *4*, 6.
31. Ibrahim, R.M. A Review on Online-Banking Security Models, Successes, and Failures. In Proceedings of the 2018 International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC), Tamil Nadu, India, 28–29 January 2018.
32. Khrais, L.T. Highlighting the Vulnerabilities of Online Banking System. *J. Internet Bank. Commer.* **2015**, *20*, 120. [CrossRef]
33. Poeng, K.P.; Chukwuere, J.E.; Agu, N.T. The issues affecting employees' adoption of online banking in mahikeng. In Proceedings of the 2nd International Conference on Information System and Data Mining, Lakeland, FL, USA, 9–11 April 2018; pp. 70–75. [CrossRef]
34. Hassan, M.A.; Shukur, Z. Review of Digital Wallet Requirements. In Proceedings of the 2019 International Conference on Cyber Security (ICoCSec), Negeri Sembilian, Malaysia, 25–26 September 2019; pp. 43–48. [CrossRef]
35. Karim, N.A.; Shukur, Z. Review of user authentication methods in online examination. *Asian J. Inf. Technol.* **2015**, *14*, 166–175. [CrossRef]
36. Shaju, S.; Panchami, V. BISC authentication algorithm: An efficient new authentication algorithm using three factor authentication for mobile banking. In Proceedings of the 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, India, 19 November 2016; pp. 1–5. [CrossRef]
37. Hua, J. Study on mobile E-commerce security payment system. In Proceedings of the International Symposium on Electronic Commerce and Security (ISECS 2008), Guangzhou, China, 3–5 August 2008; pp. 754–757. [CrossRef]
38. Serrano, M.E.; Godoy, S.A.; Gandolfo, D.; Mut, V.A.; Scaglia, G.J.E. A Simple Off-line E-Cash System with Observers. *Inf. Technol. Control* **2018**, *47*, 118–130. [CrossRef]
39. Omariba, Z.B.; Masese, N.B. Security and Privacy of Electronic Banking. *Kidney Int. Suppl.* **2013**, *3*, 262. [CrossRef]
40. Kang, J. Mobile payment in Fintech environment: Trends, security challenges, and services. *Hum. Cent. Comput. Inf. Sci.* **2018**, *8*, 32. [CrossRef]
41. Bahtiyar, Ş.; Gür, G.; Altay, L. Security Assessment of Payment Systems under PCI DSS Incompatibilities. In *IFIP International Information Security Conference*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 395–402. [CrossRef]
42. Khattri, V.; Singh, D.K. Implementation of an Additional Factor for Secure Authentication in Online Transactions. *J. Organ. Comput. Electron. Commer.* **2019**, *29*, 258–273. [CrossRef]
43. European Central Bank (ECB). *Recommendations for the Security of Internet Payments*; European Central Bank (ECB): Frankfurt, Germany, 2013; pp. 1–26. ISSN 978-92-899-0866-6.