BIOMETRIC BASED THREE-FACTOR MUTUAL AUTHENTICATION SCHEME FOR ELECTRONIC PAYMENT SYSTEM USING ELLIPTIC CURVE CRYPTOGRAPHY

Malathi D.[1*] and Sasikaladevi N.[2]

[1,2]School of Computing, SASTRA Deemed University, Thanjavur, Tamil Nadu, India

Email: malathi@sastra.ac.in[1*](corresponding author), sasi@cse.sastra.edu

DOI: https://doi.org/10.22452/mjcs.sp2020no1.4

ABSTRACT

Electronic payment system plays a vital role in e-commerce and other financial transactions with ever-increasing acceptance of smart device based applications. To ensure secure transactions, various authentication schemes have been proposed in recent times. But existing password and smart card-based traditional e-payment systems have some limitations and also raises security concerns. However, they consume more energy and are not feasible for the e-payment system as it consists of resource constraint devices like mobile devices. Furthermore, it is prone to security issues if the password is guessed or smart card is stolen. Thus to enhance the security and to reduce the computational cost, biometric authentication based payment protocol using elliptic curve cryptography is proposed. Since biometric features are unique and also cannot be stolen or reproduced. The proposed system resists various security attacks like impersonation attack, replay attack, session key agreement, man-in-the-middle attack, and user anonymity. Furthermore, it reduces computational and communication costs when compared to other protocols as it exploits ECC. Thus the proposed authentication protocol is convenient for the electronic payment system. A simulation tool, AVISPA is utilized to verify the security of designed payment protocol and BAN logic for formal security analysis.

Keywords: Mutual authentication, Biometrics, Elliptic Curve Cryptography, BAN Logic, AVISPA

1.0 INTRODUCTION

With the ever-growing progression of information and communication technologies, its adoption in various fields helps to ease the everyday task and makes life more convenient than ever. The growing popularity of online applications and inadequate time to purchase items promote the existence of e-commerce. In e-commerce, people are flexible in selecting brands and products of their own choice and also given the privilege to return unsatisfied products. It helps to increase the trust between customer and product sellers. In the context of commerce, the electronic payment method acts as a backbone for the rapid breakthroughs due to its accessibility, digitization, and speed. Electronic payment system supports users to shop and pay bills online by sitting at their home.

Generally, the E-payment system involves user, merchant, bank server, and authorized third party to resolve any disputes if it arises. Users are convenient enough to save time and money with the arrival of electronic payment system while using several online-based applications. For instance, online bill payment, personal transactions, loan management, online shopping and internet banking grown to a greater extent with the help of e-payment system. Nevertheless, financial transaction through the public network is vulnerable to threats and adversary may take advantage to perform several attacks to eavesdrop users' financial or personal information. Thus several authentication protocols were introduced to prevent unauthorized user access, where authentication refers to the validation of authorized users' identity [1].

Traditional authentication protocol utilizes a password or smartcard embedded with personal information and secret parameters to identify authorized users. But in the context of commerce, the traditional electronic payment system has some limitations and flawed in providing security when the password is compromised or the smart card is stolen [2]. As a result, biometric authentication is considered as an effective alternative to verify the identity of a legitimate user. Due to the unique characteristics of human biometric features, it is not easy to forge like signatures, stolen like a smart card or guess like password [3]. Thus it is used in many applications like banking, academic institutes, healthcare, identifying suspects, and also in defense. The utilization of biometric authentication in e-payment helps to prevent identity theft, reduce security issues, and also facilitates user convenience.

To reduce computational complexity, storage space, and communication cost of many existing authentication protocols, ECC (Elliptic Curve Cryptosystem) is utilized. ECC is a public key cryptosystem which provides same degree of security provided by other public key cryptosystem like RSA but with lesser key size. On the other hand, the security of ECC based protocol lies in the complexity of breaking the discrete logarithmic problem. Motivated by the above-mentioned objectives, an energy-efficient authentication protocol using ECC is proposed, which suits well for the e-payment system as it contains the resource constraint device. Thus it is capable enough to achieve essential requirements of e-payment systems such as confidentially, integrity, authenticity, non-repudiation, forward secrecy, and unforgeability.

To address the weakness and design flaws of authentication schemes discovered in the literature, we design a biometric authentication based session key agreement protocol for electronic payment system based on the elliptic curve cryptosystem. The security of the protocol is verified formally by BAN logic, and AVISPA is utilized to verify the achievement of required privacy goals. Informal security analyses were performed to show that the protocol resists several possible attacks like impersonation attack, smart card stolen attack, reply attack, and denial of service attack. It also ensures user anonymity, session key agreement, and perfect forward secrecy. Finally, computational costs were computed and compared with other related protocols to prove the improved performance of the proposed protocol.

1.1 Research contributions

The contribution of the research work is as follows:

- A secured biometric authenticated payment protocol for an electronic payment system is proposed to overcome the security limitations found in the literature. Biometric features are used to improve security properties as they are unique, unforgeable, and irreproducible.
- The security of the protocol is validated using an automated validation tool AVISPA. In addition, security against various attacks is analyzed informally and also formally through BAN logic.
- Finally, computational and communication cost is analyzed in comparison with other schemes to demonstrate the energy efficiency of the proposed protocol.

1.2 Organization of the paper

The remaining of the work is structured as follows: Section 2 gives an overview of biometric authentication-related literature in various fields. Section 3 presents the mathematical background and preliminaries for a better understanding of the proposed scheme. Section 4 describes the proposed biometric authenticated session key agreement protocol for the e-payment system. Validation is performed, and simulation results were given in section 5. Then formal security analysis is made based on BAN logic in section 6, and informal security analysis is discussed in section 7. Performance evaluation is given in section 8. Finally, in section 9, the proposed work is concluded with some future directions.

2.0 RELATED WORK

In recent times, the electronic payment system has attracted many customers due to the booming development of communication technologies. Customers can purchase anything they wish through online using mobile devices enabled with an electronic payment application. It is used for online shopping, bill payment, tax payment, bank transactions, etc. without the physical usage of actual money. Thus payment system has been incorporated in almost all online-based applications. As such, electronic payment has become an essential part of everyday life. The security and privacy are the concern which hinders the pervasive acceptance of e-payments. The major challenges of electronic payment systems are user anonymity, privacy protection, reusability, fair exchange, and forgeability.

In order to address the security challenges, key agreement and mutual authentication are essential for the E-payment system to ensure secure payments. Several authentication schemes were proposed in various fields [4-6] to ensure secure communications over a public channel. Juang [7] developed a smart-card based efficient authenticated key agreement scheme for multi-server using symmetric cryptography. But the scheme does not afford user anonymity as it transmits users' identity over the public channel and also does not withstand insider attack. Wu et al. [8] designed an authentication scheme for Telecare Medicine Information Systems (TMIS). Das and Goswami [9] present a robust biometric-based authentication system for remote users with a smart card to preserve anonymity. But they all are two-factor authentication protocols.

Besides the performance efficiency of password and smart card-based authentication schemes, researchers observed that they are susceptible to various attacks. Because some parameters stored secretly in the smart card, they are easy to eavesdrop. Several security breaches were also occurred due to loss or stolen of smart card and identifiable information. Experts from FinTech also suggest that traditional e-payment systems based on password and smart cards are lagging in providing security. Thus, to overcome the limitations of such schemes, many researchers considered biometric information as a third factor to design secured authentication protocols [10]. The advantages of using biometric features for authentication are they cannot be stolen or forgettable, difficult to reproduce, hard to forge, cannot be guessed easily, and complex to break [11, 12].

The biometric-based authentication procedure is first introduced by Yoon and Yoo [13] for a multi-server environment. Then, Chuang and Chen [14] proposed the biometric authentication based key agreement method for multi-server architecture to preserve user anonymity. But, Mishra et al. [15] argued that Chuang and Chen's scheme is insecure and projected a new biometric authentication based key agreement model. Later, Lu et al. [16] declares the flaws in Mishra et al.'s protocol and presented the robust biometric-based key agreement protocol. Nevertheless, Chaudhry [17] founds that Lu et al.'s method suffers from impersonation attack and user anonymity. Later, he developed the improved biometric-based authentication protocol for multimedia networks. Kumar et al. [18] introduced an authentication scheme for multi-server using biometrics features where the fuzzy extractor is utilized to match patterns.

Amin and Biswas [19] proposed authentication protocol with three-factor for multi-server, which is applicable for TMIS and also provides user anonymity. But, Das et al. [20] stated the design flaws of their scheme and presented a robust key agreement protocol for TMIS with user authentication. Later, Amin et al. [21] improved Das et al.'s scheme using ECC and proposed an authentication protocol, which also ensures user anonymity. Unfortunately, Irshad et al. [22] discovered that Amin et al.'s model is exposed to impersonation and password guessing attacks. Recently, Qi et al. [23] proposed the biometric authentication based key exchange protocol for TMIS using ECC. The authors stated that their work ensures perfect secrecy with user anonymity and mutual authentication. It also resists attacks like impersonation and password guessing attacks.

In the context of e-payment, Yang et al. [24] presented an authenticated encryption model using ECC in 2013. But Heydari et al. [25] declared that Yang et al.'s method undergoes impersonate attack. Later, Chaudhry et al. [26] claims the same and proposed an improved electronic payment system. They stated that their proposed scheme resists all possible attacks and also reduces the computational cost by 66%. But, Kang et al. [27] found user anonymity, dispute resolution, and fair exchange problems in Chaudhry et al.'s model and proposed an enhanced e-payment model using authenticated encryption and verifiably encrypted signature scheme. From the survey, it is observed that biometric features are essential to authenticate legal user and ECC to reduce computational overhead, which suits well for applications like e-payment systems with resource constraint devices.

3.0 MATHEMATICAL BACKGROUND AND PRELIMINARIES

Mathematical background and preliminaries used for complete understanding of the proposed biometric authenticated payment protocol is presented in this section.

3.1 Fuzzy Extractor

Biometric features are widely used to verify the legitimacy of the particular person due to its unique characteristics. At the same time, false rejections due to noise are the most accepted limitation of biometric based schemes. Fortunately, Fuzzy extractor helps to prevent false rejection in most of the biometric based authentication schemes [30]. It consists of deterministic reproduction *Rep*() and probabilistic generation *Gen*() procedures. *Gen*() procedure takes the biometric template as input and outputs an auxiliary string θ and random string σ, i.e. $Gen(B) = (\sigma, \theta)$ in an error tolerant way. Though the imprinted biometric does not matches the stored biometric templates, it authenticates the person because the random string σ remains unchanged with auxiliary string θ, i.e. $Rep(B^*, \theta) = \sigma$, which means B^* equals to B if *Rep*() can recover σ from B^* with θ.

3.2 Elliptic curve cryptography (ECC)

ECC provides comparable security with other public key cryptosystem like RSA but with smaller key size. An EC $E_p(a, b)$ over a prime field F_p is a non-singular curve which is characterize by the equation $y^2 = x^3 + ax + b \bmod p$, where $a, b \in F_p$ with the discriminate $4a^3 + 27b^2 \bmod p \neq 0$. The set of points on the elliptic curve with point at infinity together forms a group. The three basic arithmetic operations performed on ECC are scalar point addition, point multiplication and point doubling. Let $P_1, P_2 \in E(F_p)$ be two points on the curve, then $P_3 = P_1 + P_2 \bmod p \in E(F_p)$ is point addition. Pont doubling is $P_3 = P_1 + P_1 \bmod p \in E(F_p)$ i.e. addition of same point, whilst scalar multiplication is the addition of same point in k times i.e. $P_3 = kP_1 \bmod p \in E(F_p)$. The strength of using ECC in biometric authentication scheme is its complexity in solving logarithmic problem. That is, given P and Q, it is difficult to acquire an integer $\alpha \in F_p$ from $Q = \alpha \times P$.

3.3 E-payment system

In general, electronic payment system consists of three members, namely, User, Merchant and Bank server. Initially, both the participating agents register themselves with the bank server. The bank server encrypts the user credentials and embeds it in the smart card, then sends it to the particular user. Similarly, bank server encrypts merchant's credentials and keeps it secret between bank server and merchant. Then in the authentication phase, participating entities verifies others authenticity by means of bank server. For that, bank server first checks whether he/she is a legal user or not and then sends the authentication challenge to them. Likewise, the proposed mutual authentication protocol for Electronic payment system enhances the security using ECC and biometric features. General framework of the proposed biometric authentication based payment protocol is illustrated in Fig. 1.

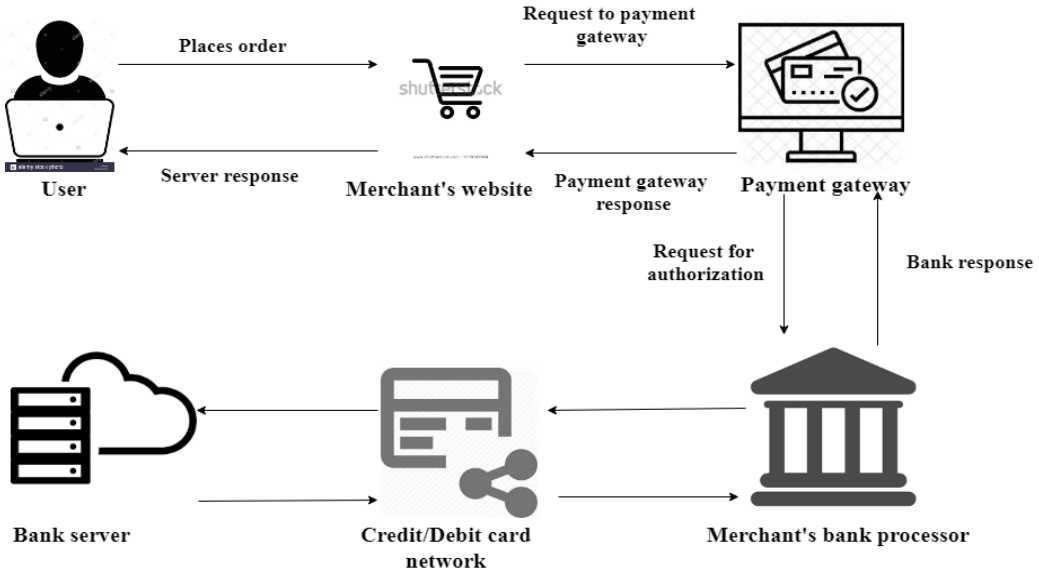

Fig. 1: General architecture of typical e-payment system

The proposed authentication scheme for e-payment consists of three phases: 1. Initialization phase, 2. Registration phase, 3. Mutual authentication and session key negotiation phase. When registered user wishes to make online payment, he sends the request with its details to the merchant for log in. Merchant forwards the user request with its own details. The bank server validates the credentials and sends the authentication message to merchantand user. Now after successful verification of challenge received from bank server, merchant computes the session key and transmits it to user with

hashed value and authentication challenge. Finally, user verifies the authentication challenge and generates hash value for computed session key. If it matches, it means that session key is successfully negotiated between user and merchant.

In this protocol, Elliptic curve cryptosystem is used as it provides equal level of security comparable to RSA but with smaller key size. The key size of 256-bit ECC is comparable to 3072-bit RSA and it is 10000 times stronger than 2048-bit RSA key. Since it has smaller key size, communication cost is low. It also consumes minimal processing power and memory resulting in faster response time. And also provides Perfect Forward Secrecy which is a key advantage of ECC. Hence, we used ECC in our system to make it lightweight and energy efficient. To boost the security of proposed scheme, fuzzy extractors are used to extract biometric information. It provides key generation from biometric features and noisy data.

3.4 Security Requirements

During electronic transactions, confidential information is transmitted over public network. Thus, payment system necessitates robust cryptographic mechanism to ensure integrity, confidentiality, mutual authentication, privacy, non-repudiation, fair exchange and double spending prevention.

- **Authentication:** Participating entities like user, merchant and bank server should authenticate each other to prevent unauthorized access and false transactions.
- **Integrity:** Integrity refers to the modification or alteration of transmitting messages. Integrity should be maintained throughout the entire session.
- **Confidentiality:** Confidentiality means that certain transactional information must be known only to desired person and hidden from others.
- **Availability:** An authorized user should avail services even if it is subjected to Denial-Of-Service (DOS) attacks.
- **Perfect Secrecy:** Even in the case of new joining or departure of existing smart devices, previously communicated messages or future messages must not known to them.
- **Freshness:** It ensures that every session has fresh information and any information from previous messages is not echoed.
- **Authorization:** It ensures that only authorized person can access and provide information.
- **Preserve Privacy:** Every participant should access only their desired information not other details. Similarly, bank should know only about the billing amount not item details. But, the outsider should not access any information about the transactions and items.

4.0 BIOMETRIC BASED AUTHENTICATION PROTOCOL FOR E-PAYMENT

The proposed ECC based biometric authentication scheme for electronic payment system consists of three phases, namely, initialization phase, registration phase, and mutual authentication and session key negotiation phase. Detailed depiction on each phase is presented in the subsequent subsections. The symbols used in the authentication protocol along with its definition are presented in the Table 1 for better readability.

Table 1: Symbols used in the authentication protocol

Symbols	Description
E_p	Elliptic curve over prime field *Fp*
U_i, M_j, *BS*	Online User, Merchant and Bank Server
ID_i, PW_i, BIO_i	Users' identity, password and biometric features
PR_i, PU_i	Users' private and public key
ID_j, PW_j, BIO_j	Merchants' identity, password and biometric features
PR_j, PU_j	Merchants' private and public key
S_k, R_k	Bank servers' private and public key
Ee, *Ff*	Random Nonce
P	Base point
SM_i	Users' smart card embedded with secret parameters
Qq, *Xx*, *Ww*, *Yy*	Authentication challenge
Key	Session key
DID_i, DID_j	Masked identity of user and merchant
Gen()	Generate function
Rep()	Reproduce function
H()	Hash function
$\oplus$	Bit-wise XOR operation
||	Concatenation

4.1 Initialization phase

Bank server (*BS*) initially selects an elliptic curve $E_p(a,b)$ with base point *P* of large prime order *n*. Then generates private key $S_k \in Z_n$ and calculate its public key as $R_k = S_k \times P$. Finally, establishes the global parameters $\{E_p(a,b), P, R_k, H(\cdot)\}$ publicly. Here, $H(\cdot)$ denotes the one way hash function.

4.2 Registration phase

To ensure secure transactions, it is essential to have legal user and merchant. For that reason, both user and merchant should register legally with the bank server before any transaction takes place. Else, if any dispute arises, it is hard to resolve those disputes. Thus registration phase consists of two steps, namely, user registration and merchant registration. As revealed in Fig. 2, merchant and user register with *BS* as follows:

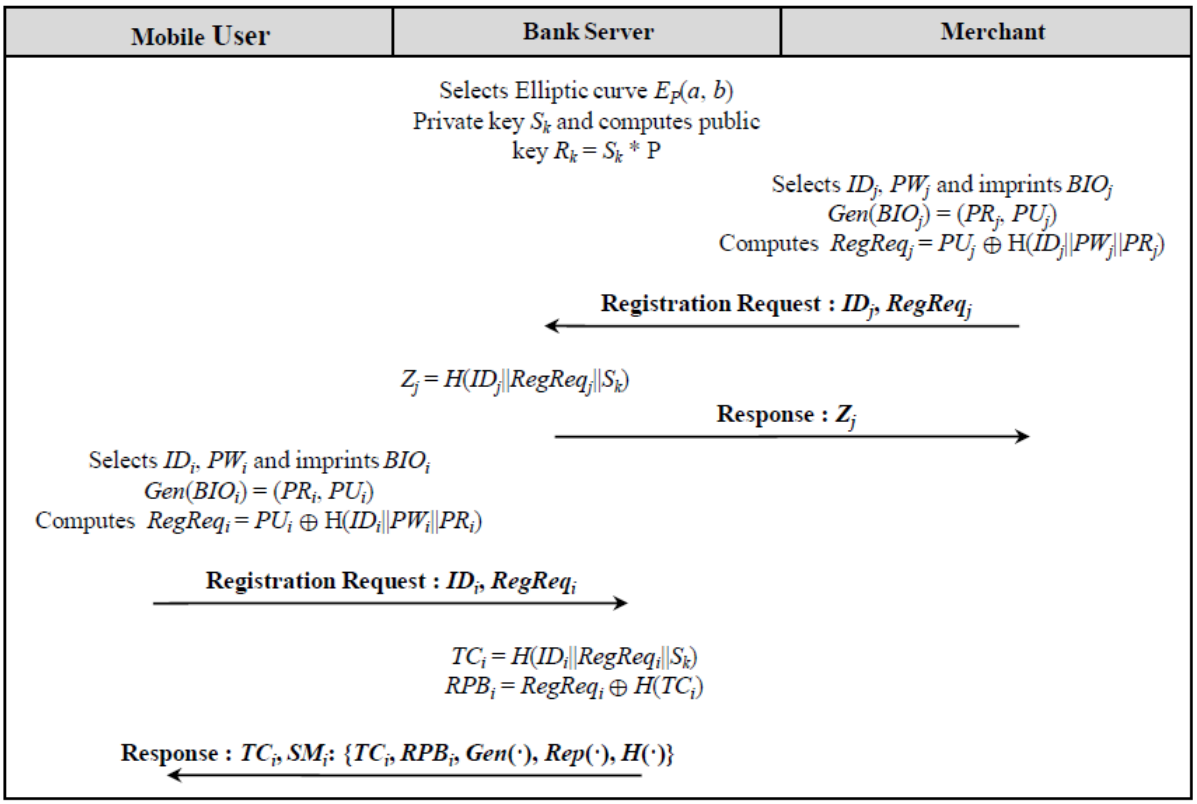

Fig. 2: Registration Phase

4.2.1 User Registration Phase

Each user *U*, initially register themselves with Bank server *BS* in this phase by sending request with information like identity, password and biometric features as follows:

- User U_i selects his own identity ID_i, password PW_i and imprints biometric BIO_i on the sensor device to compute $Gen(BIO_i) = (PR_i, PU_i)$ where $Gen(\cdot)$ is a generate function of fuzzy extractor and (PR_i, PU_i) are private and public key respectively.
- With the help of key pair, user U_i creates the request message as $RegReq_i = PU_i \oplus H(ID_i \| PW_i \| PR_i)$. Now, U_i transmits the request {*IDi* and $RegReq_i$} to *BS* securely.
- When *BS* receives the registration request from U_i, it computes $TC_i = H(ID_i \| RegReq_i \| S_k)$ where S_k is a secret key and $RPB_i = RegReq_i \oplus H(TC_i)$, then embeds {$TC_i$, RPB_i, $Gen(\cdot)$, $Rep(\cdot)$, $H(\cdot)$} in the smartcard SM_i and sends through secure channel.

4.2.2 Merchant Registration Phase

Like users, each merchant M_j register themselves with Bank server *BS* with their details for the establishment of session key and mutual authentication as follows:

- Merchant M_j chooses its unique identity ID_j, password PW_j and imprints biometric BIO_j to compute the request message $RegReq_j = PU_j \oplus H(ID_j \| PW_j \| PR_j)$ and sends the registration request {ID_j, $RegReq_j$} to *BS* via secure channel.

- *BS* computes $Z_j = H(ID_j \| RegReq_j \| S_k)$ and sends it to merchant using Key Exchange Protocol (IKEv2). Merchant keeps it secret.

4.3 Mutual authentication and Session Key Establishment

To buy some goods from any merchant, both user U_i and merchant M_j requires to confirm the authenticity among each other as shown in Fig. 3 for successful negotiation of session key.

- U_i inserts his card into a smartcard reader and inputs ID_i, PW_i and also imprints the biometric BIO_i at the sensor device. Then card reader computes $Rep(BIO_i, PU_i) = PR_i$, $M_i = PU_i \oplus H(ID_i \| PW_i \| PR_i)$ and verify whether $M_i \oplus H(TC_i)$ matches with RPB_i. If it holds then persists the process, else ejects the smartcard and terminates the session.
- After successful verification, smartcard generate fresh nonce $Ee \in Zn$ and establish $Ei = Ee*P$ and $Eia = Ee * R_k$, where $R_k = S_k * P$ is a bank server's master public key. To prevent known session temporary information attack, smartcard generates *Ei* and *Eia* instead of directly using random nonce *Ee*. Furthermore, it also computes masked identity $DID_i = ID_i \oplus H(Eia_x)$ and verification challenge $Qq = H(ID_i \| Ei \| TC_i)$. Finally, U_i transmits the request $Msg_1 = \{DID_i, Ei, Qq\}$ to merchant M_j via public channel.
- After receiving $Msg_1 = \{DID_i, Ei, Qq\}$ from U_i, M_j generates a random nonce $Ff \in Zn$ and computes $Fj = Ff * P$, $Fja = Ff * R_k$, masked identity $DID_j = ID_j \oplus H(Fja_x)$ and verification challenge $Xx = H(DID_i \| Ei \| Qq \| Fj \| Z_j)$. Finally, M_j sends legal user verification message $Msg_2 = \{DID_j, Fj, Xx, DID_i, Ei, Qq\}$ to *BS*.
- Now *BS* checks whether both user and merchant are valid registered user or not. After getting $Msg_2 = \{DID_j, Fj, Xx, DID_i, Ei, Qq\}$ from M_j, *BS* first computes $F_j * S_k = (Fja_x, Fja_y)$ then gets ID_j from $ID_j = DID_j \oplus H(Fja_x)$. BS retrieves merchants' Z_j from the database and checks whether received *Xx* equals to $H(DID_i \| Ei \| Qq \| Fj \| Z_j)$.
- Similarly, *BS* checks whether *Qq* equals to $H(ID_i \| Ei \| TC_i)$ by getting ID_i from $ID_i = DID_i \oplus H(Eia_x)$, where $E_i * S_k = (Eia_x, Eia_y)$. If both the challenge holds, then *BS* continues the session else terminates the session.
- Finally, *BS* computes the authentication challenge for both user and merchant as $Ww = H(BID_j \| ID_i \| ID_j \| Eia_x \| TC_i)$, where $BID_j = ID_j \oplus H(Eia_x)$ and $Yy = H(AID_i \| ID_i \| ID_j \| Fja_x \| Z_j)$, where $AID_i = ID_i \oplus H(Fja_x)$, respectively. Now *BS* sends the message $Msg_3 = \{AID_i, Yy, BID_j, Ww\}$ to merchant.
- Now M_j gets the identity of user U_i from AID_i as $ID_i = AID_i \oplus H(Fja_x)$ and verifies whether an authentication challenge *Yy* matches $H(AID_i \| ID_i \| ID_j \| Fja_x \| Z_j)$ or not. If holds, merchant generates session key $Key = H(ID_i \| ID_j \| Ff * Ei)$ and computes $Tt = H(Key \| ID_i)$. Finally, M_j sends the message $Msg_4 = \{BID_j, Ww, Fj, Tt\}$ to service requested user U_i.
- User U_i gets the identity of merchant from BID_j as $ID_j = BID_j \oplus H(Eia_x)$ and verifies the authentication challenge *Ww* equal to $H(BID_j \| ID_i \| ID_j \| Eia_x \| TC_i)$ or not. If holds, then generates $Key = H(ID_i \| ID_j \| Ee * Fj)$ and verifies whether generated session key is correct or not by comparing the received *Tt* with $H(Key \| ID_i)$.

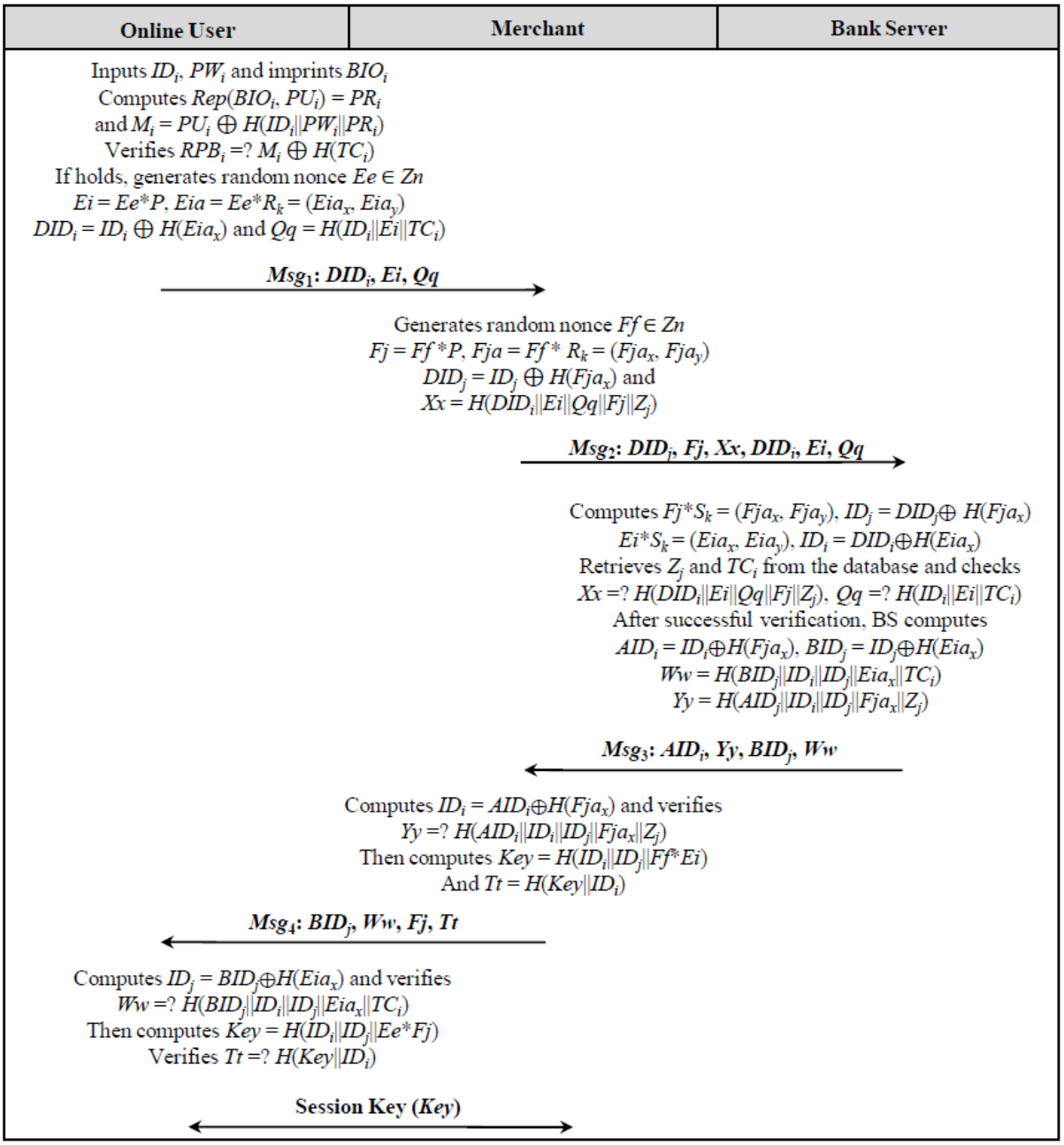

Fig. 3: Mutual Authentication and Session Key Establishment

5.0 PROTOCOL VERIFICATION USING AVISPA

In this section, an automated validation tool AVISPA is utilized to verify the security of proposed e-payment protocol for authentication. A role-oriented language, HLPSL (High-Level Protocol Specification Language) is employed to execute the scheme in AVISPA. HLPSL2IF translator converts the code into intermediate format and simulation is performed with one of the four backend checkers. The validation results demonstrate the security of authentication protocol against passive and active attacks.

5.1 Protocol Specification

The proposed biometric authenticated protocol for electronic payment system consists of three agents, namely, user U_i, merchant M_j and bank server *BS*. The role specified by the agent user U_i is given in Fig. 4. U_i initially sends the registration request $\{ID_i, RegReq_i\}$ to *BS* securely through the function $Snd(\cdot)$, which uses the Dolev-Yao attacker model. User keeps PW_i and PR_i as secret and shares ID_i with bank server. Then receives the smart card from the *BS* embedded with secret parameters. During login phase, after successful verification of biometric information, smart card generates fresh nonce *Ee* and sends login request Msg_1 to merchant through public channel. Here *Ee* is known only to user and TC_i is known to both bank server and user. The witness(·) statement says that U_i generates *Ee* freshly for *BS*. In authentication phase, U_i receives Msg_4 from merchant and verifies the computed session key *Key*.

```
role user (
 Ui, Mj, BS: agent,
 PUi, PUj, Rk: public_key,
 Mul, H: hash_func,
 Snd, Rcv: channel(dy))
played_by Ui def=
 local
  State: nat,
  IDi, PWi, PRi, RegReqi, IDj, PWj, PRj, RegReqj, Zj, Sk, TCi, RPBi, Ee, Ei,
   Eia, P, DIDi, Qq, Ff, Fj, Fja, DIDj, Xx, AIDi, BIDj, Yy, Ww, Key, Tt: text,
  Gen, Rep: hash_func
  const user_bank, merchant_bank, bank_merchant, bank_user,
   merchant_user, s1, s2, s3, s4, s5, s6, s7, s8, s9: protocol_id
 init
  State := 0
 transition
  1. State = 0 /\ Rcv(start) =|>
     State':=1 /\ RegReqi' := xor(PUi, H(IDi.PWi.PRi))
     /\ Snd(IDi.RegReqi')
     /\ secret({PWi, PRi}, s1, Ui)
     /\secret({IDi}, s2, {Ui, Mj, BS})
  2. State = 1 /\ Rcv(TCi.RPBi.Gen.Rep.H) =|>
     State':=2 /\ Ee' := new()
     /\ Ei' := Mul(Ee'.P) /\ Eia' := Mul(Ee'.Rk)
     /\ DIDi' := xor(IDi, H(Eia')) /\ Qq' := H(IDi.Ei.TCi)
     /\ Snd(DIDi'.Ei.Qq')
     /\ secret({Ee'}, s8, Ui)
     /\ witness (Ui, BS, user_bank, Qq')
  3. State = 2 /\ Rcv(BIDj.Ww.Fj.Tt) =|>
     State':=3 /\ Key':= H(IDi.IDj.Mul(Ff.Ei))
end role
```

Fig. 4: HLPSL code specification for the role played by user U_i

The role played by merchant M_j is given in Fig. 5. In registration phase, M_j convey the registration request $\{ID_j, RegReq_j\}$ to bank server securely through the function $Snd(\cdot)$ and receives Z_j through $Rcv(\cdot)$ function. Merchant keeps PW_j and PR_j as secret and shares ID_j with bank server. When it receives the service request $Rcv(DID_i, Ei, Qq)$ from any user, it generates fresh nonce *Ff* and forwards the received message with its information for verification. In authentication phase, M_j receives Msg_3 from BS and computes the session key *Key* after verifying the authentication challenge *Yy*. Then sends the Msg_4 containing authentication challenge received from *BS* with session key verification parameter *Tt* to user.

```
role merchant (
 Ui, Mj, BS: agent,
 PUi, PUj, Rk: public_key,
 Mul, H: hash_func,
 Snd, Rcv: channel(dy))
played_by Mj def=
 local
  State: nat,
  IDi, PWi, PRi, RegReqi, IDj, PWj, PRj, RegReqj, Zj, Sk, TCi, RPBi, Ee, Ei,
   Eia, P, DIDi, Qq, Ff, Fj, Fja, DIDj, Xx, AIDi, BIDj, Yy, Ww, Key, Tt: text,
  Gen,Rep: hash_func
  const user_bank, merchant_bank, bank_merchant, bank_user,
   merchant_user, s1, s2, s3, s4, s5, s6, s7, s8, s9: protocol_id
 init
  State :=0
 transition
  1. State = 0 /\ Rcv(start) =|>
     State':=1 /\ RegReqj' := xor(PUj, H(IDj.PWj.PRj))
     /\ Snd(IDj.RegReqj')
     /\ secret({PWj, PRj}, s3, Mj)
     /\ secret({IDj}, s4, {Ui, Mj, BS})
  2. State = 1 /\ Rcv(Zj) /\ Rcv(DIDi.Ei.Qq') =|>
     State':=2 /\ Ff' := new()
     /\ Fj' := Mul(Ff'.P) /\ Fja' := Mul(Ff'.Rk)
     /\ DIDj' := xor(IDj, H(Fja')) /\ Xx' := H(DIDi.Ei.Qq.Fj.Zj)
     /\ Snd(DIDj'.Fj.Xx.DIDi.Ei.Qq')
     /\ secret({Ff'}, s9, Mj)
     /\ witness (Mj, BS, merchant_bank, Xx')
  3. State = 2 /\ Rcv(AIDi.Yy.BIDj.Ww) =|>
     State':=3 /\ Key':= H(IDi.IDj.Mul(Ff.Ei)) /\ Tt':= H(Key'.IDi)
     /\ Snd(BIDj.Ww.Fj.Tt')
     /\ witness(Mj, Ui, merchant_user, Tt')
end role
```

Fig. 5: HLPSL code specification for the role played by merchant M_j

The role played by the bank server *BS* is given in Fig.6. At first, it receives the registration request $Rcv(ID_i, RegReq_i)$, $Rcv(ID_j, RegReq_j)$ from both user and merchant, respectively. Then it generates secret parameters TC_i, RPB_i, $Z_j$and sends them, which are used later for session key generation and mutual authentication. In authentication phase, *BS* receives the user verification message Msg_2: $\{DID_j, Fj, Xx, DID_i, Ei, Qq\}$ from the merchant. After successful verification of both user and merchants' identity, BS computes the authentication challenge *Yy* and *Ww* for merchant and user respectively and sends the message Msg_3: $\{AID_i, Yy, BID_j, Ww\}$ to merchant for session key negotiation. The witness(·) statement indicates the authentication between user and bank server, merchant and bank server.

```
role bankserver (
 Ui, Mj, BS: agent,
 PUi, PUj, Rk: public_key,
 Mul, H: hash_func,
 Snd, Rcv: channel(dy))
played_by BS def=
 local
  State: nat,
  IDi, PWi, PRi, RegReqi, IDj, PWj, PRj, RegReqj, Zj, Sk, TCi, RPBi, Ee, Ei,
   Eia, P, DIDi, Qq, Ff, Fj, Fja, DIDj, Xx, AIDi, BIDj, Yy, Ww, Key, Tt: text,
  Gen,Rep: hash_func
  const user_bank, merchant_bank, bank_merchant, bank_user,
   merchant_user, s1, s2, s3, s4, s5, s6, s7, s8, s9: protocol_id
 init
  State :=0
 transition
  1. State = 0 /\ Rcv(IDj.RegReqj) =|>
     State':=1 /\ Zj' := H(IDj.RegReqj.Sk)
     /\ Snd(Zj')
     /\ secret({Sk}, s5, BS)
     /\ secret({Zj}, s6, {Mj, BS})
  2. State = 1 /\ Rcv(IDi.RegReqi) =|>
     State':=2 /\ TCi' := H(IDi.RegReqi.Sk)
     /\ RPBi' := xor(RegReqi.H(TCi))
     /\ Snd(TCi'.RPBi'.Gen.Rep.H)
     /\secret({TCi}, s7, {Ui, BS})
  3. State = 2 /\ Rcv(DIDj.Fj.Xx.DIDi.Ei.Qq) =|>
     State':=3 /\ AIDi' := xor(IDi, H(Fja))
     /\ BIDj' := xor(IDj, H(Eia))
     /\ Yy' := H(AIDi'.IDi.IDj.Fja.Zj)
     /\ Ww' := H(BIDj'.IDi.IDj.Eia.TCi)
     /\ Snd(AIDi'.Yy'.BIDj'.Ww')
     /\ witness (BS, Mj, bank_merchant, Yy')
     /\ witness (BS, Ui, bank_user, Ww')
end role
```

Fig. 6: HLPSL code specification for the role played by bank server *BS*

The HLPSL code for the session role and environment is presented in the Fig. 7 with authentication goals. Role session declares all variables and Snd/Rcv channel for all agents. Role environment specifies all global constants, intruder knowledge, sessions and goals. After successful implementation of proposed authentication protocol in HLPSL code, HLPSL2IF converter is executed to convert the HLPSL code to IF code to visually observe the execution of authentication protocol.

```
role session (
 Ui, Mj, BS: agent,
 PUi, PUj, Rk: public_key,
 Mul, H: hash_func)
def=
 local T1, R1, T2, R2, T3, R3: channel(dy)
 composition user(Ui, Mj, BS, PUi, PUj, Rk, Mul, H, T1, R1)
 /\ merchant(Ui, Mj, BS, PUi, PUj, Rk, Mul, H, T2, R2)
 /\ bankserver(Ui, Mj, BS, PUi, PUj, Rk, Mul, H, T3, R3)
end role

role environment()
def=
 const ui, mj, bs: agent,
 pui, puj, rk: public_key,
 mul, h: hash_func,
 idi, pwi, pri, regreqi, idj, pwj, prj, regreqj, zj, sk, tci, rpbi, ee, ei,
  eia, p, didi, qq, ff, fj, fja, didj, xx, aidi, bidj, yy, ww, key, tt: text,
 user_bank, merchant_bank, bank_merchant, bank_user,
  merchant_user, s1, s2, s3, s4, s5, s6, s7, s8, s9: protocol_id
 intruder_knowledge={ui, mj, bs, mul, h}
composition
 session(ui, mj, bs, pui, puj, rk, mul, h)
end role
goal
 secrecy_of s1
 secrecy_of s2
 secrecy_of s3
 secrecy_of s4
 secrecy_of s5
 secrecy_of s6
 secrecy_of s7
 secrecy_of s8
 secrecy_of s9
 authentication_on user_bank
 authentication_on merchant_bank
 authentication_on bank_merchant
 authentication_on bank_user
 authentication_on merchant_user
end goal
environment()
```

Fig. 7: HLPSL code specification for the role session and environment

5.2 Simulation Results

AVISPA consists of OFMC, CL-AtSe, SATMC and TA4SP backend checkers. The proposed biometric based authenticated protocol for e- payment is simulated under OFMC and CL-AtSe backend checkers. Simulation results given

in Figs. 8 and 9 demonstrates that proposed protocol is safe and secure against passive and active attacks. The first section of both the backend checker is SUMMARY, where security of the protocol is concluded as safe, inconclusive or unsafe. Second section depicts the DETAILS of the protocol, which sates on which condition the protocol is safe, or under which condition it finds an attack or the reason for inconclusive. The remaining section gives the name of the protocol, goals attained, name of the backend checker, then comments and statistics about attacks if traced.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/testsuite/results/PS.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.20s
  visitedNodes: 7 nodes
  depth: 3 plies
```

Fig. 8: Result of OFMC backend checker

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/testsuite/results/PS.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 0 states
  Reachable  : 0 states
  Translation: 0.07 seconds
  Computation: 0.00 seconds
```

Fig. 9: Result of CL-AtSe backend checker

6.0 FORMAL SECURITY ANALYSIS USING BAN LOGIC

Security features of the designed biometric authentication based payment protocol are analyzed precisely using widely-accepted Burrows-Abadi-Needham logic and illustrate that it ensures mutual authentication. The BAN logic includes set of inference rules and notations to validate freshness, message source and trustworthiness of protocol which are summarized as follows:

6.1 Notations of BAN logic:

- $P \mid\equiv X$: P believes the message X.
- $P \lhd X$: P sees X.
- $P \mid\sim X$: P once said X.
- $P \Rightarrow X$: P has jurisdiction over X.
- $P \overset{k}{\leftrightarrow} Q$: P and Q share the same key k.
- $\{X\}_k$: X is encrypted with key k.
- $\#(X)$: X is freshly generated.

6.2 Inference Rules of BAN logic:

Message Meaning Rule (MMR): $$\frac{P \mid\equiv P \overset{k}{\leftrightarrow} Q, P \lhd \{X\}_k}{P \mid\equiv Q \mid\sim X}$$

Nonce Verification Rule (NVR): $\frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$

Freshness-Conjuncatenation Rule (FCR): $\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$

Jurisdiction Rule (JR): $\frac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$

Session Key Rule (SKR): $\frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\equiv X}{P \mid\equiv P \overset{k}{\leftrightarrow} Q}$

6.3 Protocol Verification

With the help of following goals and assumptions, authentication of the protocol is demonstrated and successful establishment of session key.

Step 1: Consider the following authentication goals.

Goal 1: $U_i \mid\equiv M_j \equiv U_i \overset{Key}{\longleftrightarrow} M_j$

Goal 2: $U_i \mid\equiv U_i \overset{Key}{\longleftrightarrow} M_j$

Goal 3: $M_j \mid\equiv U_i \equiv U_i \overset{Key}{\longleftrightarrow} M_j$

Goal 4: $M_j \mid\equiv U_i \overset{Key}{\longleftrightarrow} M_j$

Step 2: The idealized form of messages communicated over public network are as follows:

Message 1: $U_i \rightarrow M_j : DID_i, Ei, Qq$

Message 2: $M_j \rightarrow BS : DID_j, Fj, Xx, DID_i, Ei, Qq$

Message 3: $BS \rightarrow M_j : AID_i, Yy, BID_j, Ww$

Message 4: $M_j \rightarrow U_i : BID_j, Ww, Fj, Tt$

Step 3: Further, some assumptions are defined as follows:

Assumption 1: $U_i \mid\equiv U_i \overset{TC_i}{\leftrightarrow} BS$

Assumption 2: $M_j \mid\equiv M_j \overset{Z_j}{\leftrightarrow} BS$

Assumption 3: $U_i \mid\equiv U_i \overset{Eia_x}{\leftrightarrow} BS$

Assumption 4: $M_j \mid\equiv M_j \overset{Fja_x}{\leftrightarrow} BS$

Step 4: By using above stated assumptions and BAN logic rules, the procedure to prove mutual authentication is as follows:

From Message 1: $U_i \rightarrow M_j : DID_i, Ei, Qq$, we get

$M_j \triangleleft DID_i, Ei, Qq : \langle Qq \rangle TC_i$

By applying message meaning rule, we get

$M_j \mid\equiv U_i \mid\sim DID_i, Ei, Qq : \langle Qq \rangle TC_i$

From Message 2: $M_j \rightarrow BS : DID_j, Fj, Xx, DID_i, Ei, Qq$ and by message meaning rule, we get

$BS \mid\equiv M_j \mid\sim DID_j, Fj, Xx, DID_i, Ei, Qq : \langle Qq \rangle TC_i, \langle Xx \rangle Z_j$

From assumptions 1 and 2, we get

$BS \mid\equiv U_i \mid\equiv DID_i, Ei, Qq : \langle Qq \rangle TC_i$ and $BS \mid\equiv M_j \mid\equiv DID_j, Fj, Xx : \langle Xx \rangle Z_j$

By believing rule, BS believes both Qq and Xx because

$BS \mid\equiv Qq : \langle Qq \rangle TC_i$ and $BS \mid\equiv Xx : \langle Xx \rangle Z_j$

From Message 3: $BS \rightarrow M_j : AID_i, Yy, BID_j, Ww$ and message meaning rule, we get

$M_j \mid\equiv BS \mid\sim AID_i, Yy, BID_j, Ww : \langle AID_i \rangle Fja_x$

From assumption 5 and Jurisdiction rule, we get

$M_j \mid\equiv U_i \xleftrightarrow{Key} M_j$

We successfully proved the achievement of required privacy goals by BAN logic models. Thus the proposed protocol ensures session key agreement and mutual authentication.

7.0 INFORMAL SECURITY ANALYSIS

Biometric authentication schemes are still secure, even if an intruder gets password or smart card information. Specifically, biometric authentications are more secure than two factor authentication protocols and also resist various attacks. Security of the proposed protocol is analysed informally as follows:

7.1 User Anonymity

In login phase, user shares his real identity to merchant through $DID_i = ID_i \oplus H(Eia_x)$ and merchant sends $DID_j = ID_j \oplus H(Fja_x)$ to bank server. But without knowing Eia_x and Fja_x, an intruder cannot get the real identity of both user and merchant. Though, an intruder knows E_i, F_j and P, it is hard to compute Ee and Ff from Ei and Fj respectively, as it relies on breaking Discrete Logarithmic problem of EC (ECDLP). Similarly, after successful verification of user's and merchant's legitimacy, bank server shares the identity of the user and merchant with authentication challenge to merchant and user through $AID_i = ID_i \oplus H(Fja_x)$ and $BID_j = ID_j \oplus H(Eia_x)$ respectively. Here also, ECDLP helps to provide anonymity.

7.2 Mutual Authentication

It is essential to authenticate communicating parties before session key generation or any financial transactions. In the proposed scheme, Bank Server helps to authenticate user and merchant. At first, bank server authenticates both user and merchant by validating $Qq = H(ID_i \| Ei \| TC_i)$ and $Xx = H(DID_i \| Ei \| Qq \| Fj \| Z_j)$. Since Qq contains TC_i which is known only to user and bank server. Likewise, Xx contains Z_j which is known only by merchant and bank server. If it holds, then bank server generates the authentication challenge $Yy = H(AID_i \| ID_i \| ID_j \| Fja_x \| Z_j)$ and $Ww = H(BID_j \| ID_i \| ID_j \| Eia_x \| TC_i)$, and then sends to merchant and user respectively for future verification. With the help of Ww, user authenticates bank server and merchant. Similarly, with the help of Yy, merchant authenticates user and bank server. It depicts that proposed protocol achieves mutual authentication among user, bank server and merchant.

7.3 Session Key Agreement

During authentication, merchant computes $Key = H\left(ID_i \| ID_j \| Ff * Ei\right)$ for secure transactions. But the computed session key is not communicated directly with the user. From the service response received from the merchant, user generates the session key $Key = H\left(ID_i \| ID_j \| Ee * Fj\right)$. If it is matches the key generated by merchant, it means that no attack is performed. To verify the equality, integrity and confidentiality of session key, user computes $Tt = H\left(Key \| ID_i\right)$ and compares with *Tt* received from merchant. If it holds, session key negotiated are safe and communication begins, else the session terminates.

7.4 Unlinkability or Session Key Secrecy

The proposed protocol ensures unlinkability as it generates new key for each session. This is because, it contains *Ee* and *Ff* which are unique and freshly generated nonce. Since, it is hard for an opponent to guess or reproduce current session key by knowing previous session keys. Thus session keys are completely different from each other and by knowing previous sessions key, security of the current session key is not compromised.

7.5 Perfect Forward Secrecy

During authentication phase, both user and merchant agree with shared session key. If an adversary intends to compute session key, he needs real identity of user and merchant along with fresh nonce *Ee* and *Ff*. As we know well that it is hard to solve ECDLP, thus it is complex to get *Ee* and *Ff* from *Ei* and *Fj* respectively. Thus without knowing these parameters, it is difficult to figure session key. It shows that proposed authentication scheme ensures perfect forward secrecy.

7.6 Denial of Service attack

The legitimacy of user is first validated using smart card by computing $Rep\left(Bio_i, PU_i\right) = PR_i$, $M_i = PU_i \oplus H\left(ID_i \| PW_i \| PR_i\right)$ and verify whether $RPB_i = M_i \oplus H\left(TC_i\right)$ or not. If holds then authentication and session key generation process proceeds, else smart card rejects the session. After successful login of user, no parameter is needed to synchronize smart card, merchant and bank server. So, it concludes that the proposed scheme ensures resistance against denial of service attack.

7.7 Impersonation Attack

An opponent has to generate $Msg_1 : \{DID_i, Ei, Qq\}$ to impersonate user, for that he needs $Qq = H\left(ID_i \| Ei \| TC_i\right)$, but TC_i embedded in smart card is familiar only to user and bank server. Though smart card is stolen by opponent, without *Ee*, it is hard to get user id from $DID_i = ID_i \oplus H\left(Eia_x\right)$. It demonstrates that our scheme resists impersonation attack. Similarly, without knowing Z_j and *Ff*, an adversary cannot impersonate merchant.

7.8 Man-in-the-middle attack

An adversary has to clear all authentication challenges like $Qq = H\left(ID_i \| Ei \| TC_i\right)$, $Xx = H\left(DID_i \| Ei \| Qq \| Fj \| Z_j\right)$, $Ww = H\left(BID_j \| ID_i \| ID_j \| Eia_x \| TC_i\right)$ and $Yy = H\left(AID_j \| ID_i \| ID_j \| Fja_x \| Z_j\right)$ to perform Man-in-the-middle attack. For that, an adversary needs secret parameters TC_i, Z_j, *Ee* and *Ff*. Obviously, these are not possible as TC_i and Z_j are known only to user and merchant respectively, *Ee* and *Ff* are fresh random nonce which varies in every session. Furthermore, as adversary is unable to perform replay attack, he is also incapable to perform man-in-the-middle attack.

7.9 Offline password guessing attack

Suppose that adversary acquires users' smart card and extracts embedded secret parameters such as $TC_i = H\left(ID_i \| RegReq_i \| S_k\right)$ and $RPB_i = M_i \oplus H\left(TC_i\right)$ by side channel attack. Then to guess user's password, he

needs users' identity ID_i and biometric data Bio_i to recover PR_i from $Rep\left(Bio_i, PU_i\right) = PR_i$. Thus it is impossible to get user's biometric data and identity, it resulting in resistance to offline password guessing attack.

7.10 Privileged Insider Attack

During registration, user sends $\left\{ID_i, RegReq_i\right\}$ to bank server. Here $RegReq_i = PU_i \oplus H\left(ID_i \| PW_i \| PR_i\right)$, where PR_i is derived from $Gen\left(B_i\right) = \left(PR_i, PU_i\right)$. And the parameters ID_i, PW_i and PR_i are prevented from theft by hash function. Hence, it is impossible to get password or biometric data of legal user. Furthermore, a privileged insider cannot compute $RegReq_i$ due to unique characteristics of PR_i and one way hashing. Thus, the proposed system resists privileged insider attack.

7.11 Replay Attack

Let us assume that an opponent tries to impersonate user or merchant by intercepting the message $Msg_1 : \left\{DID_i, Ei, Qq\right\}$ or $Msg_2 : \left\{DID_j, Fj, Xx, DID_i, Ei, Qq\right\}$ and replaying back. Then during verification, bank server terminates the session as computed $Qq = H\left(ID_i \| Ei \| TC_i\right)$ or $Xx = H\left(DID_i \| Ei \| Qq \| Fj \| Z_j\right)$ is not equal to received Qq or Xx. This is because, TC_i inside the Qq and Z_j inside the Xx are known only to corresponding user or merchant and bank server. Moreover without knowing proper nonce Ee and Ff, an adversary cannot able to generate valid session key. Similarly, user or merchant will be aware of replay attack by verifying the correctness of $Ww = H\left(BID_j \| ID_i \| ID_j \| Eia_x \| TC_i\right)$ and $Yy = H\left(AID_i \| ID_i \| ID_j \| Fja_x \| Z_j\right)$.By this way, the proposed scheme resists replay attack.

8.0 PERFORMANCE ANALYSIS

Performance evaluation of biometric authentication based payment protocol is presented in the following subsections. Analyses were performed and compared with existing protocols by means of security properties and computational cost to assess the improved performance efficiency of proposed protocol.

8.1 Security Analysis

Comparative analysis of security and functionality features of proposed scheme with another scheme is shown in Table 2. It clearly depicts the attacks resisted by proposed protocol and other existing protocols. The proposed biometric based protocol provides additional security like password guessing attack, replay attack, impersonation attack, known session key temporary information attack and insider attack. Furthermore, it resists active and passive attacks verified through AVISPA tool and also we have done the popular BAN logic validation to demonstrate that our protocol achieves mutual authentication.

Table 2: Informal security analysis in comparison with other related schemes

Security attacks	Heydari et al.	Chaudhry et al.	Kang et al.	Kumar et al.	Proposed
User Anonymity	×	×	×	×	✓
Mutual Authentication	✓	×	✓	✓	✓
Session key agreement	✓	×	✓	✓	✓
Unlinkability	×	×	×	×	✓
Perfect forward secrecy	✓	×	×	×	✓
Denial of service attack	✓	✓	✓	×	✓
Impersonation attack	✓	×	✓	✓	✓
Man-in-the-middle attack	✓	×	×	×	✓
Offline password guessing attack	✓	×	×	×	✓
Privileged insider attack	✓	✓	×	×	✓
Reply attack	✓	✓	✓	✓	✓

8.2 Computational Cost Analysis

Since registration of user and merchant with bank server is carried out only once, the cost of registration is not considered much. But the cost of authentication phase is estimated and analysed with other protocols to assess the efficiency of proposed protocol. Time taken to complete one hash function is less than that of modular exponentiation, whilst encryption/decryption operations are 3 times costlier than hash function. And time taken for XOR operation is negligible. Comparison of computation cost of other protocols with proposed protocol is given in Table 3. To make computational cost comparison with other schemes, the following notations are used to define the computational time required to perform one particular operation:

T_E: Modular Exponentiation
T_M: EC Scalar Point Multiplication
T_A: EC Point Addition
T_H: Hash Function
T_S: Symmetric Encryption/Decryption
T_I: Inversion

From table 3, it is observed that cost of proposed protocol is comparatively lower than other related protocols. Hence, it is concluded that proposed protocol is energy efficient in terms of computational cost.

Table 3: Computational cost comparison with other related protocols

Scheme	Computational cost
Yang et al. [24]	$8T_{PM} + 7T_{E/D} + 2T_H + 2T_{DS}$
Heydari et al. [25]	$4T_{PM} + 7T_{E/D} + 2T_H + 2T_{DS} + 3T_M + 2T_I$
Chaudhry et al. [26]	$4T_{PM} + 7T_{E/D} + 2T_H + 2T_{DS} + 3T_M + 2T_I$
Kang et al. [27]	6TPM + 9E/D + 2TH + 2TDS + TM + TI
Kumar et al. [28]	$12T_M + 4T_A + 8T_S + 6T_H + 8T_{DS}$
Proposed Scheme	$8T_M + 18T_H$

9.0 CONCLUSION

At present, electronic payments act as a backbone and key component for many online-based applications like e-commerce and e-banking. But data security and user's privacy are the major concern of any payment system. Existing authentication protocol consumes more energy and lacks security. Moreover, as e-payment is performed on resource-constrained devices, it is essential to design a light-weight protocol. ECC is used to minimize the computation and communication costs of the payment system. Thus, a secured authentication protocol for e-payment is proposed using ECC and biometric features. The proposed authentication protocol is enhanced to meet security requirements like unlinkability, anonymity, and perfect forward secrecy. The performance analysis of the authentication protocol is performed in comparison with existing schemes in two aspects, namely, the number of cryptographic operations used in the protocol and security features. The comparative analysis demonstrates the enhanced results over other schemes. Further, simulation results of AVISPA ensure that the proposed protocol withstands both passive and active attacks like man-in-the-middle attack, replay attack, etc. And BAN logic is used to prove that our scheme ensures secure authentication formally. Finally, a discussion on informal security analysis also illustrates that our scheme resists various malicious attacks. As a result, the proposed authentication scheme is energy efficient and appropriate for real-time applications like the e-payment system. In the future, we planned to exploit other public-key cryptosystems to reduce much more storage space and energy without compromising the security level.

ACKNOWLEDGEMENT

The authors are grateful to Science and Engineering Research Board (SERB), Department of Science and Technology, New Delhi, for the financial support under ECR grant (ECR/2017/000679/ES). Authors also thank SASTRA University, Thanjavur, for providing the infrastructural facilities to carry out this research work.

REFERENCES

[1] A. Hovav, & R. Berger, "Tutorial: identity management systems and secured access control". *Communications of the Association for Information Systems*, Vol. 25, No. 1, 2009, pp. 42.

[2] D. Abrazhevich, "Electronic payment systems: A user-centered perspective and interaction design". *Dennis Abrazhevich*, 2004.

[3] R. Clodfelter, "Biometric technology in retailing: Will consumers accept fingerprint authentication?". *Journal of Retailing and Consumer Services*, Vol. 17, No. 3, 2010, pp. 181-188.

[4] Y. P. Liao, & S. S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment". *Computer Standards & Interfaces*, Vol. 31, No. 1, 2009, pp. 24-29.

[5] M. K. Khan, S. K. Kim, & K. Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'". *Computer Communications*, Vol. 34, No. 3, 2011, pp. 305-309.

[6] X. Li, J. Ma, W. Wang, Y. Xiong, & J. Zhang, "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments". *Mathematical and Computer Modelling*, Vol. 58, No. 1-2, 2013, pp. 85-95.

[7] W. S. Juang, "Efficient multi-server password authenticated key agreement using smart cards". *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 1, 2004, pp. 251-255.

[8] Z. Y. Wu, Y. C. Lee, F. Lai, H. C. Lee, & Y. Chung, "A secure authentication scheme for telecare medicine information systems". *Journal of medical systems*, Vol. 36, No. 3, 2012, pp. 1529-1535.

[9] A. K. Das, & A. Goswami, "A robust anonymous biometric-based remote user authentication scheme using smart cards". *Journal of King Saud University-Computer and Information Sciences*, Vol. 27, No. 2, 2015, pp. 193-210.

[10] C. T. Li, & M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards". *Journal of Network and computer applications*, Vol. 33, No. 1, 2010, pp. 1-5.

[11] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards". *IET Information Security*, Vol. 5, No. 3, 2011, pp. 145-151.

[12] A. K. Das, & A. Goswami, "A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care". *Journal of medical systems*, Vol. 37, No. 3, 2013, pp. 9948.

[13] E. J. Yoon, & K. Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem". *The Journal of supercomputing*, Vol. 63, No. 1, 2013, pp. 235-255.

[14] M. C. Chuang, & M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics". *Expert Systems with Applications*, Vol. 41, No. 4, 2014, pp. 1411-1418.

[15] D. Mishra, A. K. Das, & S. Mukhopadhyay, "A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards". *Expert Systems with Applications*, Vol. 41, No. 18, 2014, pp. 8129-8143.

[16] Y. Lu, L. Li, X. Yang, & Y. Yang, "Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards". *PLoS One*, Vol. 10, No. 5, 2015, e0126323.

[17] S. A. Chaudhry, "A secure biometric based multi-server authentication scheme for social multimedia networks". *Multimedia Tools and Applications*, Vol. 75, No. 20, 2016, pp. 12705-12725.

[18] S. Kumari, A. K. Das, X. Li, F. Wu, M. K. Khan, Q. Jiang, & S. H. Islam, "A provably secure biometrics-based authenticated key agreement scheme for multi-server environments". *Multimedia Tools and Applications*, Vol. 77, No. 2, 2018, pp. 2359-2389.

[19] R. Amin, & G. P. Biswas, "A secure three-factor user authentication and key agreement protocol for tmis with user anonymity". *Journal of medical systems*, Vol. 39, No. 8, 2015, pp. 78.

[20] A. K. Das, V. Odelu, & A. Goswami, "A secure and robust user authenticated key agreement scheme for hierarchical multi-medical server environment in TMIS". *Journal of medical systems*, Vol. 39, No. 9, 2015, pp. 92.

[21] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, & N. Kumar, "An efficient and practical smart card based anonymity preserving user authentication scheme for TMIS using elliptic curve cryptography". *Journal of medical systems*, Vol. 39, No. 11, 2015, pp. 180.

[22] A. Irshad, M. Sher, O. Nawaz, S. A. Chaudhry, I. Khan, & S. Kumari, "A secure and provable multi-server authenticated key agreement for TMIS based on Amin et al. scheme". *Multimedia Tools and Applications*, Vol. 76, No. 15, 2017, pp. 16463-16489.

[23] M. Qi, J. Chen, & Y. Chen, "A secure biometrics-based authentication key exchange protocol for multi-server TMIS using ECC". *Computer methods and programs in biomedicine*, Vol. 164, 2018, pp. 101-109.

[24] J. H. Yang, Y. F. Chang, & Y. H. Chen, "An efficient authenticated encryption scheme based on ECC and its application for electronic payment". *Information Technology and Control*, Vol. 42, No. 4, 2013, pp. 315-324.

[25] M. Heydari, S. Sadough, S. A. Chaudhry, M. Sabzinejad Farash, & M. R. Aref, "An Improved Authentication Scheme for Electronic Payment Systems in Global Mobility Networks". *Information Technology and Control*, Vol. 44, No. 4, 2015, pp. 387-403.

[26] S. A. Chaudhry, M. S. Farash, H. Naqvi, & M. Sher, "A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography". *Electronic Commerce Research*, Vol. 16, No. 1, 2016, pp. 113-139.

[27] B. Kang, D. Shao, & J. Wang, "A fair electronic payment system for digital content using elliptic curve cryptography". *Journal of Algorithms & Computational Technology*, Vol. 12, No. 1, 2018, pp. 13-19.

[28] R. Kumar, S. K. Pal, & A. Yadav, "Elliptic curve based authenticated encryption scheme and its application for electronic payment system". *International Journal of Computing Science and Mathematics*, Vol. 9, No. 1, 2018, pp. 90-101.

[29] A. Braeken, "An improved e-payment system and its extension to a payment system for visually impaired and blind people with user anonymity". *Wireless Personal Communications*, Vol. 96 No. 1, 2017, pp. 563-581.

[30] Y. Dodis, R. Ostrovsky, L. Reyzin, & A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data". *SIAM journal on computing*, Vol. 38, No. 1, 2008, pp. 97-139.