JOINT KEY AUTHENTICATION MODEL FOR SITUATION VARIANT IN E-HEALTH SYSTEMS

Dr. Maruf Pasha, Muhammad Sajjad
Computer Science Department

Abstract: Security & Privacy of patient in e-health systems is focal point of every stakeholder at the time of migration from traditional into electronic healthcare services. Various user authentication and authorization mechanisms are proposed and in practice to maximize security and privacy but specifically deal in criticality on the bases of types of users still questionable. Proposed model is joint authentication mechanism with situation variant in e-health systems. In this model, create flexibility in mutual key authentication mechanism using four key factors alternatively at the time of utilization of these key factors authentication according to critical situation incurred by the application users. Formal Specification of proposed authentication model is verified by the well-known HLPSL specification language using AVISPA tool. This satisfiability enhances the security and privacy of e-health systems and as well as reduces the rigidness in joint key authentication model. Moreover this model has also economical and strategically edging for health care organizations and also for health care personnel.

Index Terms---- e-health systems, joint key authentication, mutual authentication, security & privacy, healthcare domain, formal specification, HLPSL, AVISPA,

Introduction:

Network communication grows sooner and quicker. It is renowned to everybody that open atmosphere is self-doubting. Attacker might use all kind of info he or she may be controlling to falsify a lawful user, or at least catch valuable data from the database. [7, 9] An isolated user verification structure theaters a vital role in forming communication over uncertain channels. Some Scholars have considered two-factor [13] confirmation structures by means of password and a retention device for over 23 years. Peoples who have the both features at the same time can login the special system. Additionally, biometrics acknowledgement becomes a general subject in the previous eras; canvassers have established three-factor [1] secluded validation schemes to improve the sanctuary of a system for smart wireless devices. By speedy development in mobile machinery, mobile devices like PDAs, Cells turn to be the retention devices in validation procedure. In latest years, numerous three factor authentication systems have been introduced. In 2009, two researchers [28] projected a three-factor verification structure along with public-key and symmetric cryptosystems. In 2010 [27] introduced a three-factor authentication system with low calculation by applying only hash function.

Related Work:

Latest development of system services, proper user recognition for isolated user validation for uncertain communication networks is progressively essential. Conflicting to customary password-based remote user verification, biometrics-based verification has better security and is supplementary reliable for remote user verification [6]. In addition, three-factor confirmation systems have been projected in many books. Biometrics-based substantiation systems are progressively communal for isolated user identity validation systems. Due to its biological or communicative features, remote verification systems may deliver improved sanctuary by means of such methods as thumbprint authentication, iris examination, facial investigation, handwritten autograph confirmation and keystroke examination[34].

Usability of E-health systems in health care industry are emergent day by day and different health care providers, government agencies, insurance companies, patients and healthcare professionals many other stakeholders directly or indirectly getting benefits from digital world [4, 5]. Patient safety and liveness is core objective of every stakeholder but electronic healthcare systems are not trustworthy as

compare to traditional. Many internal and external threads are there, cyber crimes are there, adversary & hackers attacks are there that would be curial and hurdles for delivery of reliable healthcare services to the patients [21].

Several user authentication mechanisms [35] are in practice in which Identity password, Biometric template, Smart card, Mobile device factors individually or collectively use for user verification. But everyone has more or less pros and cons reported by the users like password break, online/offline dictionary attacks, password guessing attacks, breach in password and stolen verifier attacks while using traditional ID/PWD authentication similarly biometric template verifier attacks, breach in smart care verification, smart card stolen attacks also reported in smart card user authentication [2, 3]. These are the reasons researchers believe in mutual authentication between user and server using three key factor agreements [27].Through this way, majority e-health care systems save from above mention threads and attacks.

In health care domain, where mutual authentication using joint key factors enhance security and privacy also problematic and hectic for users in the delivery of health care services to the patients [10]. User bound to use id password, biometric template and smart card jointly while granting access into the system. But in real time scenario, there could be many problems for user to use joint key factors sometime forget password, damage or unclear biometric template, or smart card stolen and many other cases or reasons to stop the user to access e-health systems [22].

Systematic literature reviews [35] and survey and interview responses showed that users trust on authentication of system using mutual key factors but there should be reliable mechanism in which user authenticate and access the e-health systems on the bases of criticality and types of users. In short need of mutual authenticated system that deals with dynamic authentication mechanism on each distinct situation.

TABLE I
Notations & Terminology

Notation	Feature
U_i	User Healthcare personnel
BT_i, BT_i^*	Biometric Pattern or Template of Ui
ID_{SC}	Identity of Smart Card of Ui
ID_{md}	Identity of Mobile Device of Ui
ID_i	Identity of User Ui
PW_i	Password of User Ui
H(.)	Hash Function
H*(.)	Bio Hash Function
$\|\|$	String concatenation Sign
$\oplus$	XOR operator
HS	HealthCare Server
LC_i	Login Case of each User Ui
rn_i	High entropy random no
LC(.)	Login Case Function String
S_i	String of ith transmitted using transmission
Δ, τ	Biometric and other factor matching algorithm

TABLE II
Verification Relation in HealthCare Server

Biometric Identity (S_2)	LC_0	LC_i (login case dynamic string)

Proposed Methodology:

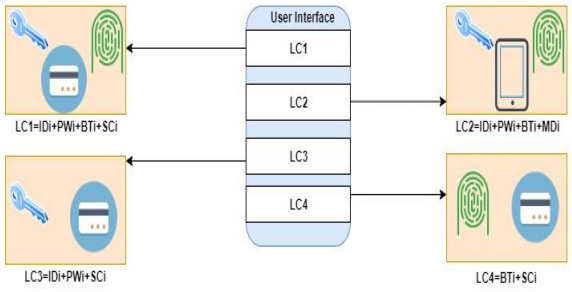

Fig. 1. In Joint Key Authentication Scheme use four factors Identity, Password, Smart Card and Mobile Device applicable in different cases alternatively to access system for user in various situations.

Registration Phase:

User Ui choose ID, PW imprint biometric template and Random no, take Hash value by applying $S_1 = H(ID_i \,||\, PW_i \,||\, H^*(BT_i))$
Encrypt biometric identity with random no 1 $S_2 = BT_i \oplus \mathrm{rn}_1$, Hash value of Identity and Password encrypted of random no 1 $S_3 = H(ID_i \oplus PW_i) \oplus \mathrm{rn}_1$ then hash value of ID, PW and Random no encrypted with S_2 and save value in S_4 string. After that Send four string S_1, S_2, S_3 and $S_4$to Healthcare Server HS.HS use its private information master key hs generate ID_{sc} for Smart Card and ID_{md} for Mobile Device. Concatenation S_2

with master key hs and extract hash value. $\mathcal{M}= H(H^*(S_2)||\, hs)$. Select random no rn_2 and then hash and encrypt $LC = H(H^*(S_2) \oplus rn_2)$ finally compute X_1 of hash value concatenation of smart card id, Master key and random no 1 for smart card $X_1 = H(ID_{sc}||S_1 \,||\, M\,) \oplus rn_2$ similarly compute X_2 of hash value concatenation of mobile device $X_2 = H(ID_{md}||S_1 \,||\, M\,) \oplus rn_2$ encrypt master key with $S_1 Y = M \oplus S_1$ store $\{S_2\,, LC_0, LC_1\}$into database of HS.

Store some strings into smart card and mobile device $\underset{\text{write into Smart Card}}{\{ID_{sc}\,,H(.),H^*(.),X_1,Y,S_3\,,S_4\}}$and $\underset{\text{write into Mobile Device}}{\{ID_{md}\,,H(.),H^*(.),X_2,Y,S_3\,,S_4\}}$ finally encrypt biometric template with random no 1 and save into smart card and mobile device.

TABLE III
Login phase with respect to alternative Key Factors

Login Case 1(ID_i/PW_i+BT_i+SC_i)	Login Case 2 (ID_i/PW_i+BT_i+MD_i)	Login Case 3 (ID_i / PW_i + SC_i))	Login Case 4 (SC_i + BT_i)
User Ui Input ID_i , PW_i , Imprint BT_i^* Choose Random no rn_3 Insert Smart Card into Card reader and compute following strings	User Ui Input ID_i , PW_i , Imprint BT_i^* Choose Random no rn_3 Attach Mobile Device with Terminal and compute following strings	User Ui Input ID_i , PW_i Choose Random no rn_3 Insert Smart Card into Card reader and compute following strings	Imprint BT_i^* Choose Random no rn_3 Insert Smart Card into Card reader and compute following strings
$S_1^* = H(ID_i \,||\, PW_i \,||\, H^*(BT_i^*)\,)$	$S_1^* = H(ID_i \,||\, PW_i \,||\, H^*(BT_i^*)\,)$	$S_3 \oplus \mathrm{rn}_1 \;=\; H(ID_i \oplus PW_i)$	$\mathrm{rn}_1 = S_3 \oplus H(ID_i \oplus PW_i)$
$M^* = Y \oplus H(S_1^*)$	$M^* = Y \oplus H(S_1^*)$	$\triangle(H(ID_i \oplus PW_i)\,,\; H(ID_i^* \oplus PW_i^*)\;) =$ □	$S_2 \;=\; H(ID_i \oplus PW_i \oplus \mathrm{rn}_1) \oplus S_4$
$rn_2^* = X_1 \;\oplus H(ID_{sc}\|\|S_1^* \,||\, M^*)$	$rn_2^* = X_2 \;\oplus H(ID_{md}\|\|S_1^* \,||\, M^*)$	$S_1^* = H(ID_i^* \,||\, PW_i^* \,||\, H^*(BT_i)\,)$	$S_2^* = BT_i^* \oplus \mathrm{rn}_1\,,\; \triangle\,(S_2^*\,, S_2) \leq$ □□
$rn_1^* = \; Z \oplus H^*(S_2)$	$rn_1^* = \; Z \oplus H^*(S_2)$	$M^* = Y \oplus S_1^*$	$S_1^* = H(ID_i \,||\, PW_i \,||\, H^*(BT_i^*)\,)$
$S_5 = H^*(BT_i^* \oplus rn_1^* \oplus rn_2^*)$	$S_5 = H^*(BT_i^* \oplus rn_1^* \oplus rn_2^*)$	$rn_2^* = X_1 \;\oplus H(ID_{sc}\|\|S_1^* \,||\, M^*)$	$M^* = Y \oplus S_1^*$
$S_6 = \; BT_i^* \oplus rn_1^* H(M^* \,||\mathrm{rn}_3)$	$S_6 = \; BT_i^* \oplus rn_1^* H(M^* \,||\mathrm{rn}_3)$	$rn_1^* = \; Z \oplus H^*(S_2)$	$rn_2^* = X_1 \;\oplus H(ID_{sc}\|\|S_1^* \,||\, M^*)$
$S_7 = \; \mathrm{rn}_3 \oplus H^*(BT_i^* \oplus rn_1^*)$	$S_7 = \; \mathrm{rn}_3 \oplus H^*(BT_i^* \oplus rn_1^*)$	$S_5 = H^*(BT_i \oplus rn_1^* \oplus rn_2^*)$	$rn_1^* = \; Z \oplus H^*(S_2)$
$\{S_5\,, S_6, S_7\}$ login request message send to HS	$\{S_5\,, S_6, S_7\}$ login request message send to HS	$S_6 = \; BT_i \oplus rn_1^* H(M^* \,||\mathrm{rn}_3)$	$S_5 = H^*(BT_i^* \oplus rn_1^* \oplus rn_2^*)$
		$S_7 = \; \mathrm{rn}_3 \oplus H^*(BT_i \oplus rn_1^*)$	$S_6 = \; BT_i^* \oplus rn_1^* H(M^* \,||\mathrm{rn}_3)$
		$\{S_5\,, S_6, S_7\}$ login request message send to HS	$S_7 = \; \mathrm{rn}_3 \oplus H^*(BT_i^* \oplus rn_1^*)$
			$\{S_5\,, S_6, S_7\}$ login request message send to HS

Authentication Phase:

On receiving $\{S_5\,, S_6, S_7\}$ login request message from U_i, HS search LC* from User Login Case Table and Obtain S_2. First of all, searches the column dynamic string (LC) and if equal to LC* then extract corresponding value S_2 searches the column Dynamic String (LC_0) and if equal to LC* Then extract corresponding value S_2 finally replace LC with LC_0 otherwise HS reject U_i login request. Suppose, S_2 has been extracted after successful comparison of dynamic strings then HS generate a Random Number rn_4,

and compute $M' = H(H^*(S_2)||\, hs) rn_3^* = S_7 \oplus H^*(BT_i^* \oplus rn_1^*)$ and$BT_i^* \oplus rn_1^* \;=\; S_6 \oplus H(M^* \,||\mathrm{rn}_3)$ compare $BT_i^* \oplus rn_1^* and S_2$ within bearable threshold,

Session terminate with if $BT_i^* \oplus rn_1^*$threshold greater than proposed valuecompute S_8 and S_9 and send to U_i $S_8 = \; rn_4 \oplus H(BT_i^* \oplus rn_1^*)\; S_9 = H((BT_i^* \oplus rn_1^*)||rn_3^*||rn_4)$

On receiving $\{S_8\,, S_9\}$ from Healthcare Server HS. $rn_4^* = \; S_8 \oplus H(BT_i^* \oplus rn_1^*) S_9 = H((BT_i^* \oplus rn_1^*)||rn_3^*||rn_4^*)$ Verifies the above string hold the value or not?

TABLE IV
Session Phase

Session Key Communication between User and Smart Card	Session Key Communication between User and Mobile Device
After Successful Verification User Computes remaining strings to build session key agreement $SesK_u = H(M^* \|\| rn_3 \|\| rn_4^*)$	After Successful Verification User Computes remaining strings to build session key agreement $SesK_u = H(M^* \|\| rn_3 \|\| rn_4^*)$
$X_{new1} = H(ID_{sc} \|\| S_1^* \|\| M^*) \oplus rn_4^*$	$X_{new2} = H(ID_{md} \|\| S_1^* \|\| M^*) \oplus rn_4^*$
U_i Send S_{10} to HS for confirmation	U_i Send S_{10} to HS for confirmation
$S_{10} = H(H^*(BT_i^* \oplus rn_1^* \oplus rn_4^*) \oplus rn_4^*)$	$S_{10} = H(H^*(BT_i^* \oplus rn_1^* \oplus rn_4^*) \oplus rn_4^*)$
After receiving S_{10} from U_i and match with following string	After receiving S_{10} from U_i and match with following string
$H\left(H^*(BT_i^* \oplus rn_1^* \oplus rn_4) \oplus rn_4\right)$	$H\left(H^*(BT_i^* \oplus rn_1^* \oplus rn_4) \oplus rn_4\right)$
Session Accept by the HS if these two values same.	Session Accept by the HS if these two values same.
$SesK_{hs} = H\left(M' \|\| rn_3^* \|\| rn_4\right)$	$SesK_{hs} = H\left(M' \|\| rn_3^* \|\| rn_4\right)$
Computes $LC_{new} = H(H^*(S_2 \oplus rn_4)$ and replace (LC_0 , LC) with (LC , LC_{new})	Computes $LC_{new} = H(H^*(S_2 \oplus rn_4)$ and replace (LC_0 , LC) with (LC , LC_{new})
For HS sends to user U_i for next login $S_{11} = H(SesK_{hs} \|\| rn_4)$ for confirmation	For HS sends to user U_i for next login $S_{11} = H(SesK_{hs} \|\| rn_4)$ for confirmation
When receive confirmation from HS user U_i compare S_{11} with $H(SesK_u \|\| rn_4)$ If user fail to compare in time or does not S_{11} in time terminate the session.	When receive confirmation from HS user U_i compare S_{11} with $H(SesK_u \|\| rn_4)$ If user fail to compare in time or does not S_{11} in time terminate the session.
Replace X_1 with X_{new1} into smart card for every next login	Replace X_2 with X_{new2} into Mobile Device for every next login

Formal Specification using HLPSL in AVISPA Tool [33]

AVISPA stands for Automated Validation of Internet Security Protocols & Applications and it also called push-button tool used to formalize authentication schemes into security protocols with their security properties using formal languages [33]. AVISPA is collection of protocol analysis techniques & libraries which ensure robust, scalable, and secure and standardize security protocols. Many organizations, such as IETF, ITU, W3C and other companies want to spread out their products and services with common, secure standards and protocols. That's why AVISPA tool is one the tools to design security protocols with its state-of-the-art library functions.The AVISPA Tool consequently deciphers (by means of the HLPSL2IF Translator) a client characterized security issue into an equal particular written in the rework based formalism Intermediate Format IF. An IF particular depicts an unbounded state progress framework agreeable to formal examination: IF determinations are naturally contribution to the back-closures of the AVISPA Tool, which actualizediverse methods to look through the comparing boundless state progress framework for states that speak to assaults on the proposed properties of the conventions. The present variant of the apparatusincorporates four back-ends: the On-the-fly Model-Checker OFMC, the Constraint-Logic-based AttackSearcher CL-AtSe, the SAT-based Model-Checker SATMC, and the TA4SP convention analyzer, which confirms conventions by actualizing tree automata in view of programmed approximations. All the back-finishes of the apparatus investigate conventions under the suppositions of flawless cryptography and that the convention messages are traded over a system that is under the control of a Dolev-Yao intruder. That is, the back-closes investigate conventions by considering the standard protocol independent, offbeat model of a dynamic interloper who controls the system be that as it may, can't break cryptography; specifically, the interloper can block messages and investigate them in the event that he has the comparing keys for decoding, furthermore, he can create messages from his insight and send them under any gathering name.

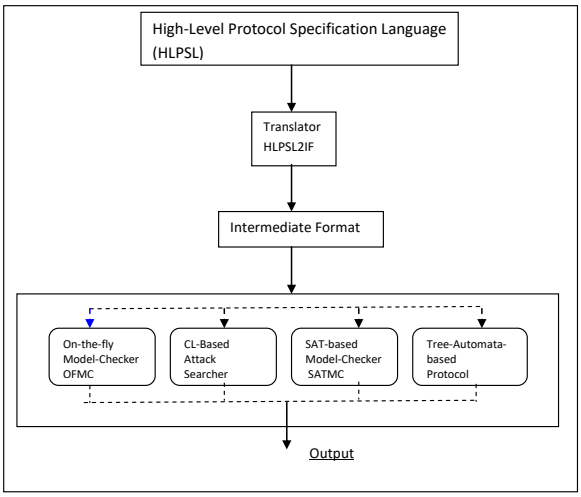

Fig. 2

HLPSL is a role-based language [33], implying that we initially indicate the succession of activities of every sort of convention member in a module, which is known as a fundamental part. This detail can later be instantiated by at least one specialists assuming the given role, and we additionally indicate how the subsequent members interface with each other by "gluing" different essential parts together into a made part. On account of the H.530 convention, for example, there are two fundamental roles, which we call user, healthcare Server, Note that role names start with lowercase letters. We use, for example, the name user to mean the role itself, while the name of the specialist assuming the role will be called Ui, as in Every essential part depicts what data the member can utilize at first (parameters), its underlying state, and manners by which the state can change (transitions). as of now showed piece of the HLPSL-determination of the healthcare Server role (and also role of the message trades of the convention in the Alice & Bob documentation), and the accompanying is the underlying piece of code

```
role user (Ui,HSJ:          agent,
           SesKuihsj        :        semmetric_key,
           H                :        hash_func,
           Hbio             :        hash_func,
           SND, RCV         :        channel(dy))
played_by Ui
def=
    local  State            :        nat,
  IDi, PWi, BTi, BTii, R1,R2,R3,R4 :          text,
  S1,S2,S3,S4,S5,S6,S7,S9,S10,S11,SesKu     :
        message,
   M,Y,Z,X1,X2,HS,IDsc,IDmd,Mi,Seskhs:    text
const   user_healthcareserver_r3,
healthcareserver_user_r4,healthcareserver_user_ses
khs,    subs1,subs2,subs3,subs4,subs5,    subs6,subs7
        :          protocol_id
init       State   :=       0
Transition
...
end role

role healthcareServer (Ui,HSJ      :        agent,
           SesKuihsj       :        semmetric_key,
           H               :        hash_func,
           Hbio            :        hash_func,
           SND, RCV        :        channel(dy))
played_by HSj
def=
    local  State           :        nat,
  IDi, PWi, BTi, BTii, R1,R2,R3,R4 :          text,
  S1,S2,S3,S4,S5,S6,S7,S9,S10,S11,SesKu     :
        message,
   M,Y,Z,X1,X2,HS,IDsc,IDmd,MiSeskhs:    text
const   user_healthcareserver_r3,
        healthcareserver_user_r4,
         healthcareserver_user_seskhs,
        subs1,subs2,subs3,subs4,subs5,  subs6,subs7
        :          protocol_id
init       State   :=       0
Transition
...
end role
```

The **Transition** segment of a HLPSL particular contains an arrangement of advances. By and large, each transition speaks to the receipt of a message and the sending of an answer message. A transition comprises of a trigger, or precondition, what's more, an activity to be performed when the activating occasion happens. For example, sample piece of code of role user in our running illustration contains the

```
Transition
% registration phase
    1.   State = 0
    /\   RCV(start) =|>
     State' :=1/\ R1' := new()
    /\  S1' := H(IDi.PWi. Hbio(BTi))
    /\  S2' := xor(BTi, R1')
    /\ S3' := xor(H(xor(IDi,PWi)),R1')
    /\ S4' := xor (H(xor (IDi,PWi,R1')),S2')
    SND({S1'.S2'.S3'.S4'}_Seskuihsj )
    secret({R1'},subs1,{Ui,HSj} )
    secret({IDi,PWi,BTi}, subs2,{Ui} )
    2.   State =1
    /\ RCV({IDsc'.X1'.Y'.S3'.S4'}_SesKuihsj)
    /\  Z= xor(R1,H(Hbio(S2)))  =|>
...
```

There is no transition in Composed roles, but instead they instantiate at least one fundamental roles, "gluing" them jointly so they execute together, ordinarily in parallel by methods for the administrator/\. That is, made roles depict **sessions** out of the protocol. In our illustration, we can characterize the accompanying made role session which instantiates one occasion of every essential role and in this manner portrays one entirety

*role **session**(Ui,HSJ:agent, SesKuihsj:semmetric_key, H: hash_func, Hbio: hash_func)*
def=
local SI,SJ,RI,RJ:channel (dy)
composition
user(Ui, HSj, SesKuihsj, H, Hbio,SI.RI)
/\ healthcareserver(Ui,HSj,SesKuihsj,H,Hbio, SJ,RJ)
end role

The final role to be characterized in a HLPSL protocol determination is a upper-level role that contains worldwide constants and an organization of at least one sessions, where the gatecrasher may assume a few roles as a real client. There is too an announcement which portrays the underlying information of the intruder. Normally, 70 L. Viganò/Electronic Notes in Theoretical Computer Science 155 (2006) 61–86
this incorporates the names of all operators, all open keys, the gatecrasher's own particular private key, any keys he imparts to others, and all openly known capacities. Note that the consistent I is utilized to allude to the gatecrasher. In our case, we could incorporate the accompanying in our HLPSL particular:

*role **environment()***
def=
const
ui,hsj:agent, seskuihsj:semmetric_key, h,hbio: hash_func,
idi, pwi, bti, btii, r1,r2,r3,r4:text
s1,s2,s3,s4,s5,s6,s7,s9,s10,s11:message,
m,y,z,x1,hs,idsc,mi,lc, seskhs:text
const user_healthcareserver_r3, healthcareserver_user_r4, healthcareserver_user_seskhs, subs1,subs2,subs3,subs4,subs5, subs6,subs7:protocol_id
intruder_knowledge = {ui,hsj,h,hbio}
composition
session (ui,hsj,seskuihsj,h,hbio)
/\ session (ui,hsj,seskuihsj,h,hbio)

end role

Security goals are indicated in HLPSL by expanding the transitions of fundamental roles with alleged goals certainties and by then allotting them an importance by portraying, in the HLPSL objective segment, what conditions — that is, the thing that mix of such actualities — show an assault. At the end of the day, we demonstrate the goals of the convention by naming a few transition in the HLPSL detail with exceptional occasions that express the significance of the progress regarding L. Viganò/Electronic Notes in Theoretical Computer Science 155 (2006) 61– 86 71 the convention objectives. For example, for mystery, the goal actualities declare which esteems ought to be mystery amongst whom, and the goal revelation in the objective area (e.g., mystery of sec m Key, sec v Key) indicates that if the gatecrasher takes in a mystery esteem that isn't unequivocally a mystery amongst him and another person, at that point the interloper has effectively assaulted the convention. Essentially, HLPSL accommodates the determination of goal certainties identified with validation (e.g., verification on key and validation on key1), which are for example used to watch that a primary is right in trusting that his proposed peer is available in the current session, has achieved a specific state, and concurs on a specific esteem, which normally is new. Inside, the assault conditions are determined as far as transient rationale (as wellbeing properties), however macros are accommodated the most as often as possible utilized security goals, i.e., mystery and distinctive types of validation (cf. the thoughts of verification talked about in

goal
secrecy_of subs1
secrecy_of subs2
secrecy_of subs3
secrecy_of subs4
secrecy_of subs5
secrecy_of subs6
secrecy_of subs7
authentication_on user_healthcareserver_r3
authentication_on healthcareserver_user_r4
authentication_on healthcareserver_user_seskhs
end goal

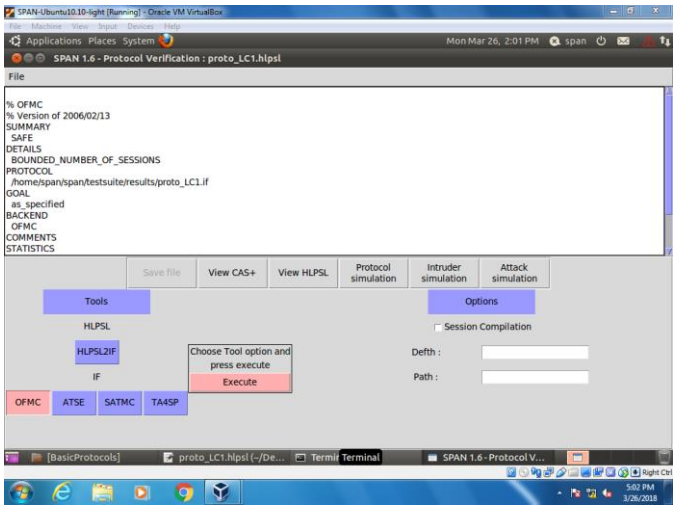

Fig. 3(a)

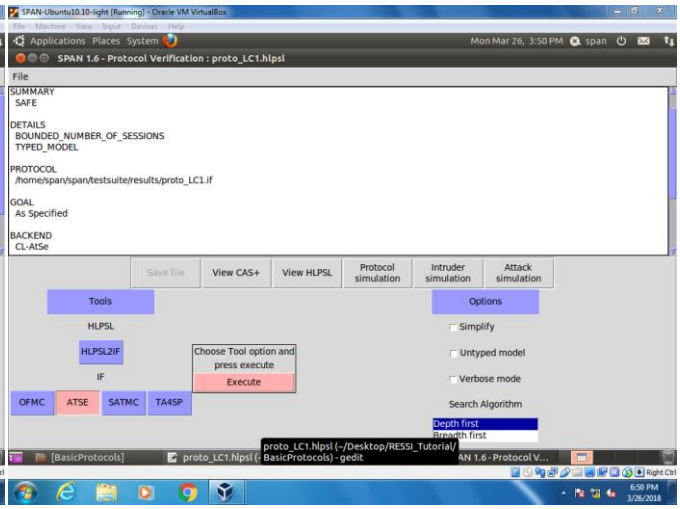

Fig. 3(b)

Informal Security Analysis on Proposed Solution

Propositions:

P1. Proposed methodology Prevent Offline password guessing Attacks

Proof: scheme resist offline password or dictionary attack i.e. suppose an Adversary A want to get the password while login from one of the login case (LC_i) did not find the IDi and PWi because transmitting messages $\{S_5 \ldots S_{11}\}$ have no info about User Ui Identity IDi and PWi. If A unfortunately obtain IDi or PWi from Smart Card $\{ID_{sc}, H(.), H^*(.), X_1, Y, S_3, S_4\}$ or from Mobile device $\{ID_{md}, H(.), H^*(.), X_1, Y, S_3, S_4\}$ but could not compute S_1 because unable to obtain values of Y and M moreover strings ciphered with high entropy random no.

P2. Proposed methodology guarantee of Biometric protection

Proof: user Ui Biometric template BTi protection wrapper with high entropy random no RN_1 and Store in Smart Card and inMobile Device in $Z = rn_1 \oplus H(H^*(S_2))$, $S_4 = H(ID_i \oplus PW_i \oplus \mathrm{rn}_1) \oplus S_2$ strings and also store in database of Healthcare server as $S_2 = BT_i \oplus \mathrm{rn}_1$ biometric identity. If Adversary A accessed on stored biometric strings but could not extract the biometric template without the knowledge of RN1 .

P3. Proposed methodology claim for User Anonymity and Untraceability

Proof: Ui store biometric identity in database, experts said that biometric identity much more difficult to expose as compare to traditional identity. Secondly while computing S_5 , S_6 , S_7 at the time of login cipher with dynamic random no RN_3 and RN4 at the time of authentication phase change in every next login the reason behind this values changes at every session and could reserve user anonymity and untraceability by the Adversary A.

P4. Proposed methodology preserve server from Insider Attack

Proof: Insider attack totally invalid in this scheme because database table did not have the identity information of Ui. HealthcareServer just store biometric template identity BTi. If Adversary A has stolen table of database unfortunately and access biometric information but this information is not useful for him/her and could not access Identity and Password of user Ui.

P5. Proposed methodology resistance to Stolen Verifier Attacks

Proof: database table consist of three attributes name Biometric Identity S_2, Login Case LC_0 and LC. If Adversary A success to steal database table and try to guesses secret key (hs) of healthcareserver and compute S2'=S6⊕h (h ((h*(S2) ||hs') ||S7 ⊕ h*(S2)) for extract verification code but in vain because threshold level of biometric template is would not be bearable threshold level. Secondly attempt to find server master key is not fruitful because master secret key extract from high-entropy random number.

P6. Proposed methodology prevent Replay Attacks

Proof: replay attack possible when communication between user Ui and healthcareserver HSi without proper authentication. To save this type of thread User Ui and Server HS communicates $\{S_5 \ldots S_{11}\}$ with mutual authentication and session key agreement. Values of RN3 and RN4 change for every next user. Suppose Adversary A trapped the communication messages between Ui and HSi and send any message to HSi and identified due to mismatch value of session key.

P7. Proposed methodology protect Impersonation Attacks

Proof: Impersonation attacks occurred when unauthorized user send messages to receiver on behalf of authorized user. This thing happen when

Adversary trace the identity of user Ui and but our proposed scheme just save biometric information in database and communicate through message with biometric identity which is infeasible for adversary to extract concrete information about legal users.

P8. Proposed methodology resist to De-synchronization Attacks

Proof: de-synchronization attacks occur when there is communication gap between Ui and HSi. In our proposed methodology HSi build session key S_{10} and send to Ui when Ui receive the session key message from HSi timely then match and compute its S_{11} as per HSi message otherwise terminate the session and restart the process of login and authentication. Proposed scheme ensure synchronization between Ui and HSi and resist such type of attacks.

P9. Proposed methodology guarantee Known Session Key Security

Proof: Known session key security persist when key computation parameter are same for both Ui and HSi. In our methodology, $SesK_{ui} = SesK_{hs}$ and use and compute M and RN_3 and RN_4 for every user and for every login session new values of high entropy random number and known by Ui and HSi. Thus proposed methodology guarantee known session key security.

P10. Proposed methodology Ensure Perfect Forward Secrecy

Proof: Assurance of perfect forward secrecy means message secrecy hold and dynamically change at every transmitting between Ui and HSi. In this way entire communication will be save from adversary. Our proposed methodology worked on this secrecy level when values store in smart card SCi, mobile device MDi or Healthcareserver HSi. If adversary has known the PWi and secret key hs and tried to compute M and S_1 but he/she just know about current message but if he/she have biometric information otherwise fail to do this.

P11. Proposed methodology works on Perfect mutual authentication

Proof: Perfect mutual authentication means complete handshaking process occur between Ui and HSi and then data communication start between them. In our scheme, with string S_8 and S_9 authenticate process between Ui and HSi. After verification of Ui and HSi share the common $SesK_u$ and $SesK_{hs}$ and update X_{new1} and X_{new2} into smart card or mobile device. In the meanwhile LC_0 also update the new value into database table.

P12. Proposed methodology provide resistance against Man-in-the-middle Attack

Proof: Our scheme defense against Man-in-the-middle attack because we block the de-synchronization attack factors, when we are communication authentication message between Ui and HSi focuses on acknowledgement message S_{10} and S_{11} if one of them is blocked due to any reason session terminate and restart login and authentication process. This thing eradicates the thread of man-in-the-middle attack.

P13. Proposed methodology defined by Formal Security Proof

Proof: our scheme formally proofed by using formal Internet security verification AVISPA tool and simulate scheme tested from many security attacks. High Level Protocol Specification Language (HLPSL) used for define secure and reliable authentication protocols. AVISPA clearly verified that proposed methodology SAFE or UNSAFE from active and passive attacks. We have used two back-end and abstract based Methods of HLPSL name On-the Fly Model Checker (OFMC) and Constraint-Logic-Based-Attack Searcher (CL-AtSe) and displayed the result in specified format.

P14. Proposed methodology protect Smart Card or Mobile Device lost Attacks

Proof: in this situation when Smart Card SCi or Mobile Device MDi lost or stolen by Adversary A, our proposed methodology will protect authentication process and secret information from offline or online guessing attacks. For complete authentication Adversary could not Compute S1=h(IDi||PWi||h(BTi)), and M=h(h*(S2)||hs) because he/she have the information about secret master key of HSi and the value generated with one way Hash function by the HSi. There are not security vulnerable whether SCi and MDi lost or stolen by someone.

TABLE V
Security Performance Comparison with existing authentication scheme

Security Characteristics	Yeh *et al*.	Wu et al.	Amin *et al*.	Li *et al*.	Zhang *et al*	Our
P1	NA	Y	Y	Y	Y	Y
P2	Y	N	N	N	Y	Y
P3	NA	Y	N	N	N	Y
P4	Y	N	Y	Y	Y	Y
P5	Y	Y	Y	Y	Y	Y
P6	Y	Y	N	Y	Y	Y
P7	N	Y	Y	Y	Y	Y
P8	N	Y	N	N	Y	Y
P9	NA	Y	Y	Y	Y	Y
P10	N	Y	N	Y	Y	Y
P11	N	Y	Y	Y	Y	Y
P12	N	Y	Y	Y	Y	Y
P13	N	Y	Y	N	Y	Y
P14	N	N	N	N	N	Y

N= NO, Y= Yes, NA= Not Applicable

Login Cases /Situation Variant Analysis

C1: User Biometric Pattern Infected due to injuries

In HealthCare domain, Biometric template (Fingerprint, Thumb scan, Iris etc) of Application User might be affected due to injure. Its physical property has changed and unable to scan its template.

In this situation our proposed authentication methodology is supportive. User can access his or her system by using ID, PW and Smart Card.

C2: User Biometric Pattern ambiguous due to any substance

In HealthCare domain, Biometric template (FingerPrint, Thumb scan, Iris etc) of Application User might be affected due to usage of substance on the fingerprint or thumb. Its physical property wrap up with any substance like oil, carbon, dust etc. In this situation our proposed authentication methodology is supportive. User can access his or her system by using ID, PW and Smart Card.

C3: User Biometric Pattern does not meet Bearable threshold level

In this situation, user imprint biometric pattern but machine has technical fault and did not capture clear image of fingerprint or iris. Due to this reason BTi image result beyond the bearable threshold level. That's why our proposed methodology allows user to login the system with ID/PW and Smart card and extract previous biometric pattern after comparing ID/PW.

C4: ID or PW forgotten situation

In this situation, User forgets ID or PW or both but there is a choice for him/her use Biometric Template and Smart Card for accessing system. in this way, it is ease for user and system as well. System access through biometric and smart card highly secure as compare to ID + PW.

C5: ID or PW disclose situation

In this situation, user considered that his/her ID, PW disclose to somewhere or thread to steal. Biometric + Smart Card authentication is another option for him/her to access system.

C6: Smart Card lost/Stolen situation

In this situation, User has lost or stolen his/her smart card but user want to access the system for immediate bases. Our proposed methodology supports him/her to access system by using another source called mobile device. Because at the time of registration, same authentication $\underbrace{\{ID_{sc}, H(.), H^*(.), X_1, Y, S_3, S_4\}}_{\text{write into Smart Card}}$ and $\underbrace{\{ID_{md}, H(.), H^*(.), X_1, Y, S_3, S_4\}}_{\text{write into Mobile Device}}$ strings stored into smart card and mobile device so that it would be suitable alternative of smart card. Secondly usage of mobile device only for login case 2 in which user wants to access the system without using of smart card. All authentication strings extract and match from mobile devices.

C7: Smart Card damage situation

In this situation, user intentionally or unintentionally damaged his/her smart card. Our proposed methodology supports him/her to access system by using another source called mobile device. Because at the time of registration, same authentication strings stored into smart card and mobile device so that it would be suitable alternative of smart card.

C8: Smart Card Reader/Writer Problem

In this situation, smart card reader device has some electrical or mechanical defaults and unable to read card. Our scheme leads user to use his/her mobile device and access system.

C9: Mobile Device lost/Stolen Situation

In this situation, User has lost or stolen his/her mobile device but user want to access the system for immediate bases. Our proposed methodology supports him/her to access system by using another source called smart card. Because at the time of registration, same authentication strings stored into smart card and mobile device so that it would be suitable alternative of mobile device.

C10: Mobile device damage situation

In this situation, user intentionally or unintentionally damaged his/her mobile device. Our proposed methodology supports him/her to access system by using another source called smart card. Because at the time of registration, same authentication strings stored into smart card and mobile device so that it would be suitable alternative of mobile device.

C11: Mobile device detect or non-detect situation

In this situation, Mobile device did not detect by the system or user unable to read authentication info from mobile device. Our proposed methodology gives priority to use smart card in case of LC1, LC3 and LC4 for accessing system.

C12: To Impose Organizational Policy and Standard

Our proposed methodology flexible for those organizations whose define their system authentication policy and standard and also predefine login authentication factors. This scheme dynamically mold according to organization standard. Some org want their employee to access system by using ID/PW + Biometric + Mobile Device or to access system by using ID/PW + Biometric + Smart Card

C13: To manage Economical Suite

Our proposed methodology support for those organizations whose set their login factors according to current economical situation? Sometime issuance of smart card for every employee expensive as compare to mobile device , or sometime usage of biometric machines are not economical then our proposed scheme work dynamically as per the desire condition.

Table VI
Cases/Situation Variant Comparison with existing authentication Schemes

Login Cases/Situations	**Yeh *et al.***	**Wu et al.**	**Amin *et al.***	**Li *et al.***	**Zhang *et al***	**Our**
C1	NS	NS	NS	NS	NS	S
C2	NS	NS	NS	NS	NS	S
C3	NS	NS	NS	NS	NS	S
C4	NS	NS	NS	NS	NS	S
C5	NS	NS	NS	NS	NS	S
C6	NS	NS	NS	NS	NS	S
C7	NS	NS	NS	NS	NS	S
C8	NS	NS	NS	NS	NS	S
C9	NS	NS	NS	NS	NS	S
C10	NS	NS	NS	NS	NS	S
C11	NS	NS	NS	NS	NS	S
C12	NS	NS	NS	NS	NS	S
C13	NS	NS	NS	NS	NS	S

NS= NOT SUPPORTIVE S = SUPPORTIVE

Results & Discussion:

We integrated our proposed authentication (prototype) scheme with Patient Inquiry System shown in fig. 4(a,b) which was running in medium level healthcare center of locality and then examine its running and communication cost put the results in table VII and VIIIthen compare it with existing authentication schemes. We examined only the cost in term of time and space used while Login and authentication phase of Login Case 2, because registration phase conduct at once later on frequently use of login and authentication would be considerable. Development Environment used in Experiment was ASP.NET MVC 5 framework with Android Library functions and MS SQL SERVER in web-based application.

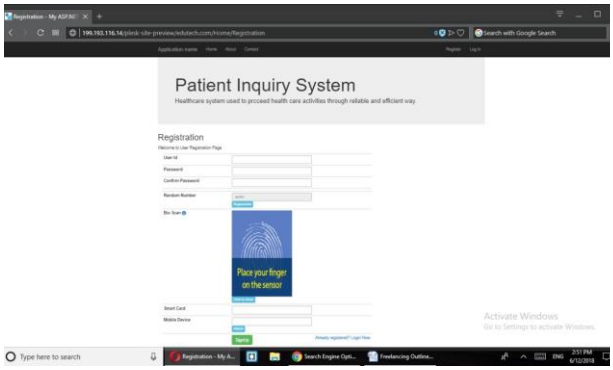

Fig. 4(a)

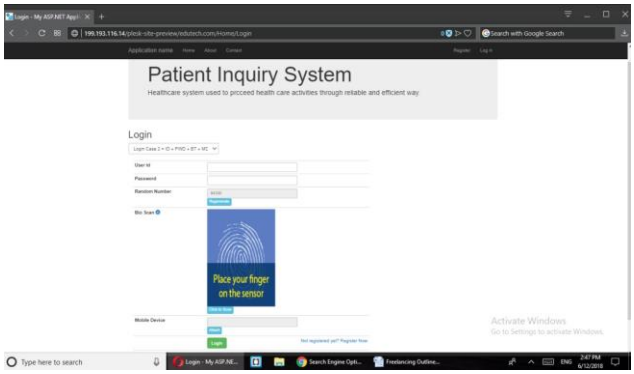

Fig. 4(b)

The selection of parameters for measure the cost of execution on the basis of consumption of highest running time, for this reason, only compute cost of Hash and Bio-hash operations which take much running time rather than XOR operation for encrypt and decrypt. Average running time showed in TABLE VIIand Fig. 5 with other existing authentication schemes. T_{hsh} and $T_{b\text{-}hsh}$ reserve to represent execution time of Hash and Bio-Hash Operations here SHA1 Hashing algorithm took to compute values. T_{sk} time for symmetric key encryption and decryption, T_{sm} timefor scalar multiplication function, T_{add} time of point of addition in elliptic curve, T_{me} time for modular exponential function.

TABLE VII
Comparison of Execution Time cost with existing authentication schemes.

Authentication Schemes	Hash & Bio Hash Opr.	Other operations used in Algorithm	Total execution Time (ms)
Yeh et al.	$3T_{hsh}$	$4T_{sm} + 12T_{add}$	3.4508
Wu et al.	$12T_{hsh} + 1T_{b\text{-}hsh}$	$4T_{sm} + 4T_{sk}$	3.2252
Amin et al.	$10T_{hsh} + 1T_{b\text{-}hsh}$	----------	0.0819
Li et al.	$10T_{hsh} + 1T_{b\text{-}hsh}$	$4T_{me}$	6.6610
Zhang et al.	$19T_{hsh} + 4T_{b\text{-}hsh}$	----------	0.0989
Our	$18T_{hsh} + 4T_{b\text{-}hsh}$	----------	0.0978

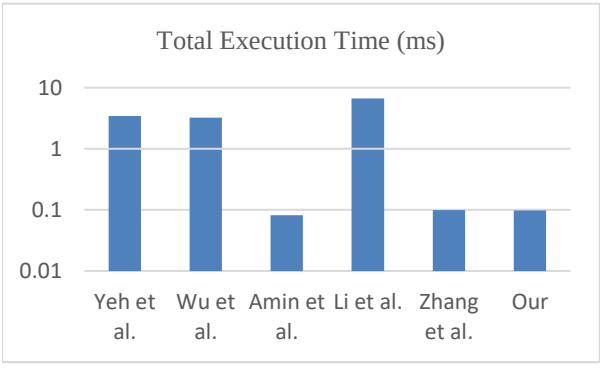

Fig. 5

As shown in table 7 that execution time (ms) in Amin et al., Zhang et al., and Our scheme is similar due to usage of same hash and bio-hash operation little bit depict the difference in number of iteration. Other Communication Cost:
Experts considered length of message in bytes while communicating among key factors, proposed scheme took output of Hash operation in 20 bytes (160 bits) and 4 bytes (32 bits) for timestamps but some other existing schemes use 32 bytes (256 bits) due to usage

TABLE VIII
Communication Cost Comparison with Existing schemes

	Yeh et al.	Wu et al.	Amin et al.	Li et al.	Zhang et al.	Our Scheme
Length (Bytes)	448	200	132	144	164	

Conclusion:

Contributions of newly proposed authentication scheme is in security and privacy mutual key factors authentication domain having dynamic behavior on selection of more than one factors while accessing the e-health systems by the users in the context of current situations. Proposed scheme is more flexible cope up real-time condition of healthcare personnel and patients want to access the system. Its dynamic behavior of selection different key factor economical for those organizations who want to adopt little bit cheap and reliable authentication mechanism. For future work, need to search more easiest and convenient ways to integrate all devices like (Smart Card Reader/Writer, Mobile Device, and Biometric Scanner) working with proposed authentication scheme. This cost reduction strategy will be encourageable for healthcare organizations and personnel for fastest acceptability of proposed authentication scheme in e-health systems.

References:

[01] Zhang, L., Zhang, Y., Tang, S., & Luo, H. (2017). Privacy Protection for E-health Systems by Means of Dynamic Authentication and Three-factor Key Agreement. *IEEE Transactions on Industrial Electronics*.

[02] L. Zhang, S. Zhu, and S. Tang, "Privacy Protection for Telecare Medicine Information Systems Using a Chaotic Map-Based Three-Factor Authenticated Key Agreement Scheme," IEEE Journal of Biomedical and Health Informatics, vol. 21, pp. 465-475, Mar 2017.

[03] J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless ensor networks," *Ad Hoc Networks*, vol. 54, pp. 147-169, Jan 2017.

authentication schemes use scalar multiplication and exponential operation using elliptic curve technique. Comparatively our scheme has low computational cost due to selection of light weight operations. of bio-hash operation with modular exponential functions rest of existing scheme given in TABLE VIII but comparatively our proposed scheme is effective due to low cost in time and space also big advantages is situation variant key factors authentication scheme.

[04] Li, X., Wen, Q., & Li, W. (2016). A three-factor based remote user authentication scheme: Strengthening systematic security and personal privacy for wireless communications. Wireless Personal Communications, 86(3), 1593-1610.

[05] Jiang, Q., Khan, M. K., Lu, X., Ma, J., & He, D. (2016). A privacy preserving three-factor authentication protocol for e-Health clouds. *The Journal of Supercomputing*, *72*(10), 3826-3849.

[06] Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., & Li, X. (2015). Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for e-health care systems. Journal of medical systems, 39(11), 140.

[07] Ling, J., & Zhao, G. (2015). An Improved Anonymous Password Authentication Scheme Using Nonce and Bilinear Pairings. IJ Network Security, 17(6), 787-794.

[08] Wu, F., Xu, L., Kumari, S., & Li, X. (2015). A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks. *Computers & Electrical Engineering*, *45*, 274-285.

[09] D. B. He and S. Zeadally, "Authentication Protocol for an Ambient Assisted Living System," IEEE Communications Magazine, vol. 53, pp. 71-77, Jan 2015.

[10] L. L. Xu and F. Wu, "Cryptanalysis and Improvement of a User Authentication Scheme Preserving Uniqueness and Anonymity for Connected Health Care," Journal of Medical Systems, vol. 39, p. 9, Feb 2015.

[11] O. Mir and M. Nikooghadam, "A Secure Biometrics Based Authentication with Key Agreement Scheme in Telemedicine Networks for E-Health Services," *Wireless Personal Communications*, vol. 83, pp. 2439-2461, Aug 2015.

[12] Islam, S. H. (2014). Provably secure dynamic identity-based three-factor password authentication scheme using extended chaotic maps. Nonlinear Dynamics, 78(3), 2261-2276.

[13] Wang, D., & Wang, P. (2014). Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks. *Ad Hoc Networks*, *20*, 1-15.

[14] M. S. Farash and M. A. Attari, "Cryptanalysis and improvement of a chaotic map-based key agreement protocol using Chebyshev sequence membership testing," Nonlinear Dynamics, vol. 76, pp. 1203-1213, Apr 2014.

[15] X. L. Li, Q. Y. Wen, W. M. Li, H. Zhang, and Z. P. Jin, "Secure Privacy-Preserving Biometric Authentication Scheme for Telecare Medicine Information Systems," Journal of Medical Systems, vol. 38, p. 8, Nov 2014.

[16] J. S. Yu, G. L. Wang, Y. Mu, and W. Gao, "An Efficient Generic Framework for Three-Factor Authentication With Provably Secure Instantiation," IEEE Transactions on Information Forensics and Security, vol. 9, pp. 2302-2313, Dec 2014.

[17] Yeh, H. L., Chen, T. H., Hu, K. J., & Shih, W. K. (2013). Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data. *IET Information Security*, *7*(3), 247-252.

[18] Yoon, E. J., & Yoo, K. Y. (2013). Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. *The Journal of supercomputing*, *63*(1), 235-255.

[19] J. L. Tsai, N. W. Lo, and T. C. Wu, "Novel Anonymous Authentication Scheme Using Smart Cards," IEEE Transactions on Industrial Informatics, vol. 9, pp. 2004-2013, Nov 2013

[20] M. K. Khan and S. Kumari, "An Improved Biometrics-Based Remote User Authentication Scheme with User Anonymity," BioMed Research International, p. 9, 2013.

[21] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," Journal of Network and Computer Applications, vol. 35, pp. 1646-1656, Sep 2012.

[22] Y. An, "Security Analysis and Enhancements of an Effective Biometric-Based Remote User Authentication Scheme Using Smart Cards," Journal of Biomedicine and Biotechnology, p. 6, 2012.

[23] X. Li, J. W. Niu, J. Ma, W. D. Wang, and C. L. Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards," Journal of Network and Computer Applications, vol. 34, pp. 73-79, Jan 2011.

[24] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," IET Information Security, vol. 5, pp. 145-151, 2011.

[25] X. Y. Huang, Y. Xiang, A. Chonka, J. Y. Zhou, and R. H. Deng, "A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, pp. 1390-1397, Aug 2011.

[26] X. X. Li, W. D. Qiu, D. Zheng, K. F. Chen, and J. H. Li, "Anonymity Enhancement on Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards," IEEE Transactions on Industrial Electronics, vol. 57, pp. 793-800, Feb 2010.

[27] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," Journal of Network and Computer Applications, vol. 33, pp. 1-5, Jan 2010.

[28] C.-I. Fan and Y.-H. Lin, "Provably Secure Remote Truly Three-Factor Authentication Scheme With Privacy Protection on Biometrics," IEEE Transactions on Information Forensics and Security, vol. 4, pp. 933-945, Dec 2009.

[29] Bhargav-Spantzel, A., Squicciarini, A. C., Modi, S., Young, M., Bertino, E., & Elliott, S. J. (2007). Privacy preserving multi-factor authentication with biometrics. Journal of Computer Security, 15(5), 529-560.

[30] Chang, C. C., & Lin, I. C. (2004). Remarks on fingerprint-based remote user authentication scheme using smart cards. ACM SIGOPS Operating Systems Review, 38(4), 91-96.

[31] Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K. (2004). Biometric cryptosystems: issues and challenges. Proceedings of the IEEE, 92(6), 948-960.

[32] Kim, H. S., Lee, S. W., & Yoo, K. Y. (2003). ID-based password authentication scheme using smart cards and fingerprints. ACM SIGOPS Operating Systems Review, 37(4), 32-41

[33] Viganò, L. (2006). Automated security protocol analysis with the AVISPA tool. Electronic Notes in Theoretical Computer Science, 155, 61-86.

[34] Brown, C. L. (2012). Health-Care Data Protection and Biometric Authentication Policies: Comparative Culture and Technology Acceptance in China and in the United States. Review of Policy Research, 29(1), 141-159.

[35] Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of biomedical informatics, 46(3), 541-562.