

به نام خدا



پیشنهاد همکاری به عنوان تک پروژه مقیم

عنوان پروژه:

طراحی و تحلیل پروتکل‌های احراز اصالت در محیط‌های منبع محدود

**Design and security analysis of authentication protocols in
resource constraint environments**

مجری:

معصومه صفخانی

بهمن ماه ۱۴۰۲

عنوان طرح: طراحی و تحلیل پروتکل‌های احراز اصالت در محیط‌های منبع محدود

مجری اصلی: دکتر معصومه صفخانی

آدرس محل کار: تهران، لویزان، دانشگاه تربیت دبیر شهید رجایی، دانشکده مهندسی کامپیوتر، گروه نرم افزار

چکیده:

با ظهور محیط‌هایی با محدودیت منبع مانند اینترنت اشیا و استفاده گسترده از آن در دنیای امروزی، یکی از چالش‌هایی که با آن روبه‌رو هستیم امنیت و حفظ حریم خصوصی است. محیط‌های با محدودیت منابع محیط‌هایی هستند که دارای محدودیت (محاسباتی، پردازشی و ذخیره‌سازی) هستند. در این خصوص طرح‌های احراز اصالت بسیاری برای تأمین دسترسی امن برای این محیط‌ها پیشنهاد شده‌است. طرح‌های احراز اصالت برای ارائه ویژگی‌های خاصی از قبیل: ناشناس بودن، غیرقابل ردیابی بودن، محرمانه بودن، دسترسی پذیری و یکپارچگی طراحی شده‌اند. از اهداف این طرح‌های امنیتی ارائه یک رویه مبادله کلید توافق شده بین کاربر و سرور یا یک دروازه است که امنیت را در برابر حملات مختلف فعال و غیر فعال مانند کشف مقادیر مخفی، ردیابی، جعل هویت، نقض یکپارچگی، حدس گذرواژه، منع خدمت و غیره را فراهم کند. ما در این پیشنهاد پروژه، تعدادی از طرح‌های امنیتی احراز اصالت ارائه شده‌ی اخیر را مورد ارزیابی قرار داده، و نقاط قوت و ضعف آنها را از نظر ویژگی‌های امنیتی، حفظ حریم خصوصی و هزینه‌های ذخیره سازی، محاسباتی و ارتباطاتی مورد بررسی قرار خواهیم داد. از طرفی آسیب پذیری پروتکل‌های ارائه شده در برابر حملات شناخته شده فعال و غیر فعال را شناسایی کرده و با ارائه راهکارهایی در راستای بهبود امنیت گام خواهیم برداشت. هم چنین امنیت آنها با استفاده از انواع روش‌های صوری و غیر صوری و نیز ابزارهای تحلیل خودکار امنیت پروتکل‌های امنیتی اثبات خواهد گردید.

کلید واژه‌ها: طرح احراز اصالت، محیط منبع محدود، توافق کلید، اینترنت اشیا، حفظ حریم خصوصی

Abstract:

With the emergence of resource-constrained environments such as the Internet of Things and its widespread use in today's world, one of the challenges we face is security and privacy. Environments with limited resources are environments that have limitations (computing, processing and storage). In this regard, many authentication schemes have been proposed to provide secure access to these environments.

Authentication schemes are designed to provide certain features such as: anonymity, untraceability, confidentiality, availability and integrity. One of the goals of these security schemes is to provide an agreed key exchange procedure between the user and the server or a gateway, which provides security against various active and passive attacks such as discovery of secret values, tracking, impersonation, integrity violation, password guessing, denial of service, and etc.

In this project proposal, we have evaluated a number of recently presented authentication security schemes, and examined their strengths and weaknesses in terms of security features, privacy protection and storage, computation and communication costs.

On the other hand, we will identify the vulnerability of the presented protocols against known active and passive attacks and take steps to improve security by providing solutions. Also, their security will be proven by using various formal and informal methods as well as automatic security analysis tools of security protocols.

Keywords: Authentication Scheme, Resource Constraint Environment, Key Agreement, Internet of Things, Privacy Protection

۱-مقدمه:

محیط‌های با محدودیت منابع به محیط‌هایی که دارای محدودیت (پردازشی، محاسباتی، ذخیره سازی) است گفته می‌شود. یکی از این محیط‌های با محدودیت منابع اینترنت اشیا است. اینترنت اشیا به‌طور کلی به اشیا و تجهیزات محیط پیرامون ما که به شبکه اینترنت متصل شده و توسط تلفن‌های هوشمند و تبلت و غیره قابل کنترل و مدیریت هستند، اشاره دارد. اینترنت اشیا به زبان ساده، ارتباط حسگرها و دستگاه‌ها با شبکه‌ای است که از طریق آن می‌توانند با یکدیگر و با کاربرانشان تعامل کنند. این مفهوم می‌تواند به سادگی ارتباط یک گوشی هوشمند با تلویزیون باشد یا به پیچیدگی نظارت بر زیرساخت‌های شهری و ترافیک باشد. این شبکه بسیاری از دستگاه‌های اطراف ما را در بر می‌گیرد. شکل ۱ نمایش‌دهنده نوعی از شبکه ارتباطی در اینترنت اشیا است. در این شکل می‌توان مشاهده کرد در این بستر هر وسیله در واقع یک موجودیت است و بسیاری از کانال‌های ارتباطی نا امن هستند. از این رو مستعد حملات فعال و غیر فعال زیادی برای نقض ویژگی‌های امنیتی هستند.



شکل ۱: مثالی از شبکه ارتباطی در اینترنت اشیا [۲]

۲-پیشینه تحقیق:

پروتکل‌های احراز اصالت و توافق کلید بسیاری نظیر [۱-۳۲] تاکنون برای محیط‌های با محدودیت منابع ارائه شده است. در واقع یک پروتکل احراز اصالت راه تعامل و ارتباطی بین موجودیت‌های مختلف به عنوان مثال کاربر و سرور است که خود شامل مراحل مختلفی است. یک پروتکل احراز اصالت امن باید بتواند در یک کانال ناامن، امنیت را تضمین کند. در این قسمت برخی از جدیدترین پروتکل‌های ارائه شده در این زمینه را شرح می‌دهیم.

^۱-Internet of Things

۲-۱ پروتکل وینود و همکاران^۱

رایانش ابری خودرویی یا VCC^۲ که یک زمینه تحقیقاتی نوظهور محسوب می‌شود شامل فناوری‌های ابری، شبکه خودرویی و اینترنت اشیا است. VCC از منابع خودرو، زیرساخت‌های ابری و محیط اینترنت اشیا استفاده می‌کند. با این حال، حفظ امنیت ارتباطات و حریم خصوصی ارتباطات دو چالش اساسی در VCC است. برای دستیابی به هدف ارتباط ایمن همراه با ناشناس ماندن، در [۱۵] یک چارچوب احراز اصالت مبتنی بر رمزنگاری منحنی بیضوی ECC را برای VCC پیشنهاد می‌کند، که مجهز به برچسب‌های شناسایی فرکانس رادیویی RFID است. این طرح احراز اصالت شامل سه مرحله است. مرحله (۱) ثبت نام، مرحله (۲) ورود و احراز اصالت و مرحله (۳) تغییر رمز عبور. در این طرح احراز اصالت از نمادها و علائمی استفاده می‌شود که در جدول ۱ نشان داده شده است.

جدول ۱: علائم و نمادهای پروتکل وینود و همکاران [۱۵]

Symbol	Description	Symbol	Description
T_i	i th RFID tag	PWT	Password of i th Tag
R_j	j th RFID reader	SL	The simulator
S	Database cloud server	x_S	Secret key of S
ID_i	The identity of i th participant	ΔT	Maximum time delay in communication
l	The security parameter	F_q	The prime finite field of order q
q	Large prime	$\oplus$	Bitwise XOR operation
$\mathcal{E}(F_q)$	Elliptic curve $\mathcal{E}$ over a prime finite field F_q	Z_q^*	Multiplicative group of order $q - 1$
G	Elliptic curve group under addition	g	Base point of G
$h(\cdot)$	Cryptographic one way hash function	$\parallel$	Concatenation operation
$SK_{ij}(\cdot)$	Session key between entities i and j	$i \stackrel{?}{=} j$	Whether i equals j
VCC	The vehicular cloud computing	sn_i	Random sequence number for i th RFID tag
E	Adversary	$\approx$	Approximate value
$i \rightarrow j : [M]$	i sends message M to j via secure channel	$i \dashrightarrow j : [M]$	i sends message M to j via public channel
RP	Registration phase	LAP	Login and authentication phase

مرحله ثبت نام در پروتکل وینود و همکاران

در این مرحله، برچسب مقادیری مانند شناسه و رمز عبور را وارد می‌کند. سپس بعد از محاسبه PWT که در روابط زیر شرح داده شده است، پیام M_{R1} در یک کانال امن به سرور ارسال می‌شود. همچنین لازم به ذکر است که مقادیر T_{R1} و T_R به ترتیب نشان دهنده عدد تصادفی تولید شده توسط برچسب و زمان جاری است.

$$PWT = h(ID_T \parallel PWT \parallel R_T)$$

$$M_{R1} = \{PWT, ID_T, T_{R1}\}$$

به محض دریافت پیام فوق، سرور زمان دریافت شده را با زمان فعلی خود مقایسه می‌کند، یعنی $T_{R2} - T_{R1} \leq \Delta T$. اگر این مقدار صحیح باشد، روند ثبت نام ادامه پیدا می‌کند در غیر این صورت متوقف می‌شود. سپس سرور یک مقدار تصادفی به نام sn_i را تولید می‌کند و مقادیر زیر توسط سرور محاسبه می‌شود.

$$X_T = h(sn_i \parallel ID_T \parallel x_S)$$

$$A_T = h(PWT \parallel X_T \parallel ID_T)$$

$$B_T = X_T \oplus PWT$$

سپس پیام $M_{R2} = \{B_T, A_T, sn_i, g, x_S, G, h(\cdot)\}$ به برچسب ارسال می‌شود.

^۱-Vinod et al.

^۲-Vehicular cloud computing (VCC)

^۳-Timestamp

بعد از دریافت پیام M_{R2} ، قرائت گرمقادیر دریافت شده، یعنی $\{B_T, A_T, sn_i, g, xs_g, G, h(.)\}$ را در حافظه خود ذخیره می‌کند. شکل ۲ روند ثبت‌نام در پروتکل وینود و همکاران را نشان می‌دهد.

Tag T_i	Cloud database server S
Inputs ID_T and pw_T Generates $R_T \in Z_q^*$ Computes $PWT = h(ID_T \ pw_T \ R_T)$ Sends $M_{R1} = \{PWT, ID_T, T_{R1}\}$ $\Rightarrow$	Verifies $T_{R2} - T_{R1} \leq \Delta T$ Generates $sn_i \in Z_q^*$ sn_i set as serial number for T_i Computes $X_T = h(sn_i \ ID_T \ x_S)$ Computes $A_T = h(PWT \ X_T \ ID_T)$ Computes $B_T = X_T \oplus PWT$ Stores sn_i corresponding to ID_T Sends $M_{R2} = \{B_T, A_T, sn_i, g, xs_g, G, h(.)\}$ $\Leftarrow$
Store $\{B_T, A_T, R_T, sn_i, g, xs_g, G, h(.)\}$ in database	

شکل ۲: مرحله ثبت‌نام در پروتکل وینود و همکاران [۱۵]

مرحله ورود و احراز اصالت در پروتکل وینود و همکاران

گام یک) برچسب مقادیر pw_T' ، ID_T' و R_T' را وارد می‌کند. سپس مقادیر زیر توسط برچسب محاسبه می‌شود:

$$PWT' = h(ID_T' \| PW_T' \| R_T')$$

$$X_T^* = B_T \oplus PWT'$$

$$A_T^* = h(PWT' \| X_T^* \| ID_T)$$

سپس مقادیر $A_T^* = A_T$ مقایسه می‌شود. در صورت صحت این رابطه روند پروتکل ادامه می‌یابد. در غیر این صورت رویه متوقف می‌شود. در صورت تساوی ذکر شده برچسب یک عدد تصادفی به نام $ag \in Z_q^*$ را تولید می‌کند و مقدار $W_1 = h(X_T^* \| ag \| ID_T)$ را هم محاسبه می‌کند و پیام M_1 که حاوی اطلاعات $\{ID_T \oplus axsg, ag, W_1, T_{LA1}\}$ است را برای قرائت‌گر ارسال می‌کند.

گام دو) قرائت‌گر مقدار تاخیر زمانی $T_{LA2} - T_{LA1} \leq \Delta T$ را بررسی می‌کند. در صورت درست بودن این مقدار، پیام $M_2 = \{ID_T \oplus axsg, ag, W_1, T_{LA3}\}$ به سرور ارسال می‌شود.

گام سه) مقدار تاخیر زمانی $T_{LA4} - T_{LA3} \leq \Delta T$ توسط سرور راستی‌آزمایی می‌شود و مقدار $ID_T^* = ID_T \oplus axsg \oplus xsag$ محاسبه می‌شود و همچنین عدد تصادفی sn_i بازیابی می‌شود. در نهایت مقدار زیر برای راستی-آزمایی $W_1 = W_1^*$ محاسبه می‌شوند.

$$X_T = h(sn_i \| ID_T^* \| X_S)$$

$$W_1^* = h(X_T \| ag \| ID_T^*)$$

همچنین در ادامه روال محاسبات سرور، سرور یک عدد تصادفی $b \in Z_q^*$ انتخاب می‌کند و مقادیر کلید نشست SK_{ST} و W_2 را محاسبه و پیام $M_3 = \{W_2, bg, T_{LA5}\}$ را به سمت قرائت‌گر ارسال می‌کند.

$$SK_{ST} = h(ID_T^* \| X_T \| bag \| xsag \| sn_i \| T_{LA5})$$

$$W_2 = h(ID_T^* \parallel SK_{ST} \parallel bg \parallel T_{LA5})$$

گام چهارم) بعد از دریافت پیام ارسالی، قرائت گر مقدار تاخیر زمانی $T_{LA6} - T_{LA5} \leq \Delta T$ را بررسی می کند و سپس پیام $M_4 = \{M_3, T_{LA7}\}$ را برای برچسب ارسال می کند.

گام پنجم) مقدار تاخیر زمانی $T_{LA8} - T_{LA7} \leq \Delta T$ توسط برچسب بررسی می شود. سپس کلید نشست SK_{TS} توسط برچسب محاسبه می گردد و مقدار W_2^* نیز مورد راستی آزمایی قرار می گیرد که در صورت صحت این مقدار، روند ورود و احراز اصالت با موفقیت به پایان می رسد.

$$SK_{TS} = h(ID_T \parallel X_T^* \parallel abg \parallel axsg \parallel sn_i \parallel T_{LA7})$$

$$W_2^* = h(ID_T \parallel SK_{ST} \parallel bg \parallel T_{LA7})$$

مرحله تغییر رمز عبور

گام یک) برچسب مقادیر ID_T' ، R_T' و PWT' را وارد می کند و سپس مقادیر زیر توسط برچسب محاسبه می شود:

$$PWT' = h(ID_T' \parallel PWT' \parallel R_T')$$

$$X_T^* = B_T \oplus PWT'$$

$$A_T^* = h(PWT \parallel X_T' \parallel ID_T')$$

سپس مقادیر $A_T^* = A_T$ مقایسه می شود. در صورت صحت این رابطه روند تغییر رمز عبور ادامه می یابد. در غیر این صورت رویه متوقف می شود.

گام دو) در این مرحله، مقدار رمز عبور همراه با یک عدد تصادفی جدید وارد می شود و سپس مقادیر زیر محاسبه می شود.

$$PWT^{NEW} = h(ID_T \parallel PWT^{NEW} \parallel R_{NEW})$$

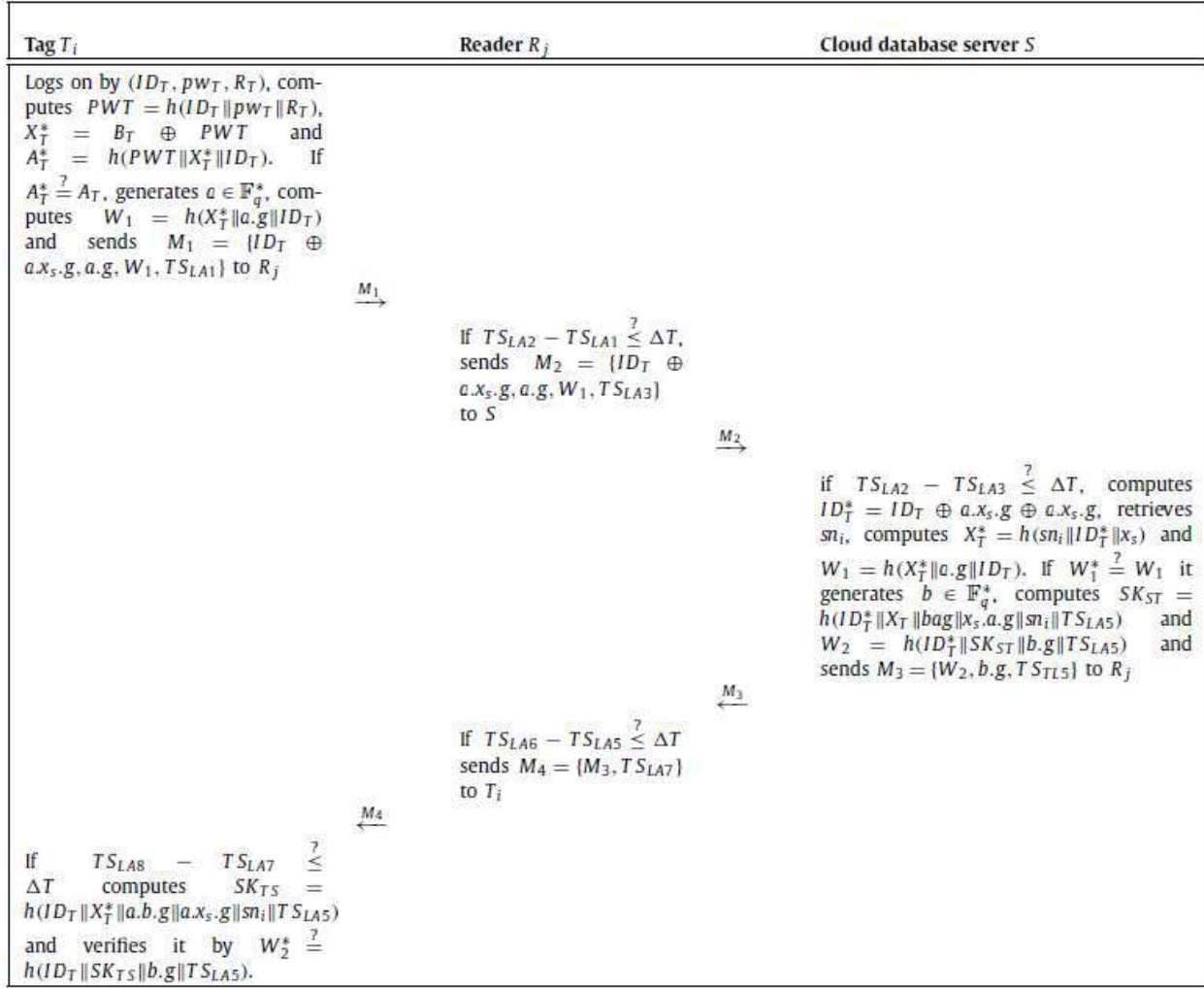
$$X_T^{NEW} = B_T \oplus PWT^{NEW}$$

گام سه) برچسب مقدار PWT را با PWT^{NEW} و PWT^{NEW} را با PWT و X_T^{NEW} را با X_T به ترتیب عوض می کند.

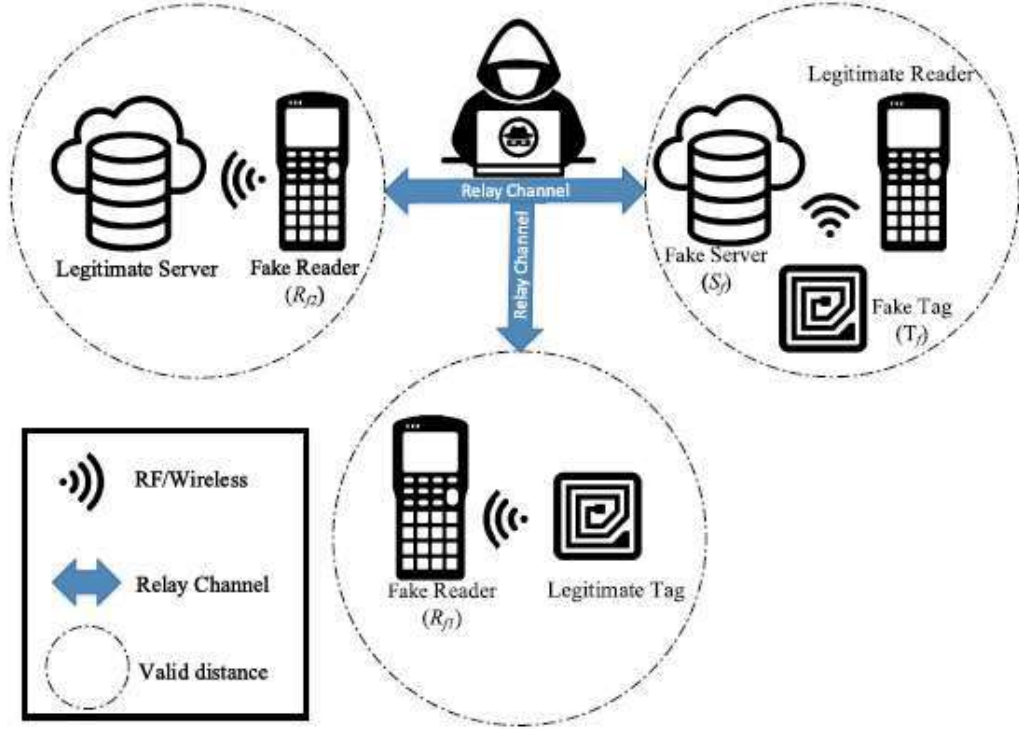
پروتکل بهبود یافته وینود و همکاران

وینود و همکاران ادعا نموده بودند که پروتکل طراحی شده آنها در برابر حملات شناخته شده ای همچون حمله تکرار، حمله جعل هویت، حمله ردیابی، حمله حدس رمز عبور خارج از خط، حمله نشست موازی، حمله غیر همگام سازی و حمله داخلی مقاوم است. ولی در [۱۶] صفحانی و همکاران نشان دادند که پروتکل [۱۵] در برابر حمله رله و حمله جعل برچسب مقاوم نیست. در شکل ۳ مرحله ورود و احراز اصالت طرح بهبود یافته وینود و همکاران [۱۶] نشان داده شده است. نکته مهم در حمله رله پیشنهادی علیه وینود و همکاران، حملات جعل هویت موفق و همچنین نقض یکپارچگی مهر زمانی مورد استفاده در پروتکل است. تحلیل امنیتی صوری پروتکل بهبود یافته با استفاده از ابزار AVISPA و نیز منطق BAN انجام شده است. در ادامه قصد داریم حمله رله و جعل برچسب ارائه شده در [۱۶] بر علیه پروتکل وینود و همکاران را شرح دهیم.

¹-Relay attack



شکل ۳: مرحله ورود و احراز اصالت پروتکل بهبود یافته [۱۶]



شکل ۴: حمله رله بین برچسب و قرائت‌گربر علیه پروتکل وینود و همکاران [۱۶]

حمله رله بر علیه پروتکل وینود و همکاران

همان طور که در شکل ۴ هم مشاهده می‌کنید فرض کنید که یک برچسب غیر مجاز در مجاورت یک قرائت‌گر مجاز قرار گرفته است و یک درخواست به صورت پیام $M_2 = \{ID_T \oplus axsg, ag, W_1, T_{LA3}\}$ را برای قرائت‌گر ارسال می‌کند. با استفاده از قرائت‌گر جعلی R_f که در مجاورت برچسب T_i قرار دارد، مهاجم این پیام را به برچسب ساختگی T_f که در مجاورت R_j قرار دارد، منتقل می‌کند.

T_f مقدار T_{LA1} را با یک مقدار مثل T'_{LA1} عوض می‌کند و سپس $M_2 = \{ID_T \oplus axsg, ag, W_1, T'_{LA1}\}$ را برای قرائت‌گر ارسال می‌کند.

قرائت‌گر R_j و سرور S برچسب را احراز اصالت می‌کنند و در پاسخ به پرس و جوی T_f ، R_j یک پیام $M_4 = \{M_3, TS_{LA7}\}$ را برای T_i ارسال می‌کند که در آن $M_3 = \{W_2, b, g, TS_{LA5}\}$ و مقدار کلید W_2 به صورت زیر محاسبه می‌شوند.

$$SK_{ST} = h(ID_T^* \parallel X_T \parallel bag \parallel xsag \parallel sn_i \parallel T_{LA5})$$

$$W_2 = h(ID_T^* \parallel SK_{ST} \parallel bg \parallel T_{LA5})$$

T_f مقدار پیام M_4 را برای R_f رله می‌کند.

R_f یک مقدار قابل قبول در پیام M_4 یعنی TS_{LA5} را با یک مقدار جعلی به صورت مثال T'_{LA7} جایگزین می‌کند و پیام M'_4 به برچسب ارسال می‌شود.

مقدار تاخیر زمانی $T_{LA8} - T'_{LA7} \leq \Delta T$ توسط برچسب مورد ارزیابی قرار می‌گیرد و در صورت صحت این زمان مقدار کلید نشست به صورت زیر محاسبه می‌شود. همچنین مقدار W_2^* راستی‌آزمایی می‌شود.

$$SK_{TS} = h(ID_T \parallel X_T^* \parallel abg \parallel axsg \parallel sn_i \parallel TS_{LA5})$$

$$W_2^* = h(ID_T \parallel SK_{ST} \parallel bg \parallel T_{LA5})$$

بر اساس حمله فوق برچسب T_i و سرور S با موفقیت کلید جلسه را به اشتراک می‌گذارند و همچنین باور می‌کنند که در مجاورت قابل قبول یکدیگر هستند در حالی که این‌طور نیست. بنابراین، دشمن با موفقیت و کارآمدی یک حمله رله را بر علیه پروتکل وینود و همکاران انجام داده است. پس از این حمله، دشمن همچنین می‌تواند پیام‌های جعلی رمزگذاری شده بین برچسب، قرائت‌گر و سرور را منتقل کند. به عنوان مثال، اگر این پروتکل برای ارتباط بین یک ماشین و یک کلید از راه دور استفاده شود، مهاجم می‌تواند به سرعت آن ماشین ذکر شده را روشن کند. همچنین در [۱۶] یک حمله رله بین سرور و برچسب نیز با استفاده از یک قرائت‌گر تقلبی یا غیرمجاز انجام شده است.

حمله جعل قرائت‌گر بر علیه پروتکل وینود و همکاران

یک مهاجم، پیام $\{ID_T \oplus axsg, ag, W_1, T_{LA1}\}$ را که از برچسب به قرائت‌گر ارسال می‌شود را می‌تواند استراق‌سمع کند. دشمن در این حین می‌تواند به جای T_{LA1} یک مقدار دیگر مانند T'_{LA1} را استفاده کند، از آنجایی که نه تنها قرائت‌گر بلکه سرور نیز یکپارچگی این مقدار را بررسی نمی‌کنند، بنابراین به مقدار زمانی مهاجم اعتماد می‌کنند، اگرچه دشمن نمی‌تواند کلید جلسه مشترک را استخراج کند، با این حال می‌تواند برچسب را جعل کند که امنیت پروتکل پیشنهادی وینود و همکاران را با خطر مواجه می‌کند.

۲-۲ پروتکل پیشنهادی کومار و چوهان^۱

در [۱۷] یک طرح آدرس‌دهی و احراز اصالت امن^۲ SCSAA مبتنی بر کارت هوشمند با اصلاح پروتکل IPV6 استاندارد برای کاهش تهدیدات امنیتی در اینترنت اشیا پیشنهاد شده است. طرح پیشنهادی دارای دو قسمت است. در مرحله اول، این طرح با اختصاص شناسه ID ۶۴ بیتی منحصر به فرد به دستگاه‌ها/لوازم هوشمند و احراز اصالت منحصر به فرد آن‌ها در شبکه اینترنت اشیا، یک روش منحصر به فرد برای آدرس‌دهی ارائه می‌دهد. در مرحله دوم، این طرح از کلید جلسه محرمانه برای جلوگیری از دسترسی غیر مجاز در شبکه استفاده می‌کند. تجزیه و تحلیل امنیت این طرح به صورت صوری با استفاده از مدل Real or Random و ابزار AVISPA انجام شده است. این تجزیه و تحلیل امنیتی ثابت می‌کند که طرح پیشنهادی از شبکه هوشمند اینترنت اشیا در برابر انواع آسیب‌پذیری‌ها و حملات مختلف محافظت می‌کند. پروتکل کومار و چوهان [۱۷] شامل ۳ مرحله است. نمادهای مورد استفاده در این پروتکل در جدول ۲ نشان داده شده است. پروتکل کومار و چوهان دارای ۱- مرحله ثبت‌نام، ۲- مرحله ورود، احراز اصالت و توافق کلید و ۳- مرحله به هنگام‌رسانی رمز عبور است.

مرحله ثبت‌نام

شکل ۵ مرحله شروع و ثبت‌نام را در پروتکل کومار و چوهان [۱۷] را نشان می‌دهد.

^۱-Pankaj Kumar, Lokesh Chouhan

^۲-Smart card based secure addressing and authentication (SCSAA)

جدول ۲: نمادها و علائم مورد استفاده در پروتکل کومار و چوهان [۱۷]

Symbol	Significance
IID_u	56-bit Interface identifier of user identity.
IID_d	8-bit Interface identifier of smart appliance/ device identity.
ID_{ug}	User gateway identity.
ID_{shs}	Smart Home server identity.
ID_{ens}	Edge node server gateway identity.
T_{id}	Time-stamp id .
$E_k[M]$	Encryption of message using secret key k.
$Token_{id}$	Short authentication token for user.
N	random nonce
U_{sid}	Pseudo identity of User
SHS_{sid}	Pseudo identity of SHS
P_{ID}	Pseudo identity of edge node server
SHS	Smart Home server.
SK	Session key
Bio_i	biometric identity of the user
PW_i	Password identity of the user
	Concatenation operation
h()	Hash function

User (U)	Edge server (ENS)
STEP 1: Chosen an identity $(ID_u \ ID_{ens} \ ID_{ug} \ T_{id})$	STEP 2 Verifies the timestamp $[(T_2 - T_1) \leq \Delta T]$ using upper bound condition, if true, it continues, otherwise, discards the session. Generates random number N chose pseudo identity P_{ID} Computes $B = h(ID_u \ N \ T_{id})$ and store (ID_u, T_{id}) in key table Assign the unique identities using <i>smart card</i> $SC = h(ID_u \ ID_d)$ and send to the user
STEP 3: Compute $C = h(B \ PW_i)$ then computes $SC = h(ID_u \ ID_d \ C)$, Compute $A = B \oplus h(PW_i \ ID_u \ T_{id})$ Compute $R = h(A \ ID_u \ T_{id} \ SC)$ Send using secret key $[E_k(R), T, N]$, where $[(T_2 - T_1) \leq \Delta T]$ send to Edge server	STEP 4 It verifies timestamp $[(T_2 - T_1) \leq \Delta T]$, if true, continue, and otherwise discard the packet. ENS computes the $(PW_i \ ID_u \ Bio_i)$ and verifies them. Then ENS verify that if $A' = A$ and verify $B' = B$, and $SC' = SC$, if true, it continues; otherwise, discard the packet. Granted the $Token_{id}$ and SK_{SHS}. Compute $B_1 = h(ID_u \ N \ T_{id}, Token_{id}, SK_{SHS})$ and send using secret key to user end to the user.

شکل ۵: مرحله شروع و ثبت نام در پروتکل کومار و چوهان [۱۷]

مرحله ورود و احراز اصالت

شکل ۶ و شکل ۷ مرحله ورود و توافق کلید را در پروتکل کومار و چوهان [۱۷] را به ترتیب نشان می دهد.

User (U)	Smart home server (SHS)
STEP 1: Insert the smart card Enter ID_u, PW_i, Bio_i Verify if $A' = A$ else verify $R' = R$ Compute $IID = h(IID_u IID_d)$ $F = h(IID PW_i, B_i)$ $M = N_1 \oplus h(F IID)$ Compute $A_1 = B \oplus h(M PW_i IID T_{id} SK_{SHS} Token_{id})$ send to the Smart home server	
	STEP 2 First it verifies the timestamp of the packet receive from user A_1 , if true, it continues, otherwise, discards the session. Generates random number N chose pseudo identity P_{ID} Computes $B = h(ID_u N T_{id} IID_u IID_d)$ and store (ID_u, T_i) in key table Granted the $Token_{id}$ and SK . Compute $B_2 = h(ID_u IID_u IID_d N T_i SK P_{ID} SHS_{sid})$ and send using secret key to user end to the user.

شکل ۶: مرحله ورود در پروتکل کومار و چوهان [۱۷]

User (U)	Smart home server (SHS)
STEP 1: Extract session key using $h(IID_u IID_d)$ Compute $K = h(U_{sid} PW_i SHS_{sid})$ Compute $S = h(IID PW_i SK N_2)$ Compute $V = S \oplus h(IID T_{id} SK N_2)$ send using secret key via open channel	
	STEP 2 SHS verifies the timestamp, $[(T_2 - T_1) \leq \Delta T]$, if it is true, then it continues, otherwise, discards the message. Compute $(U_{sid} SHS_{sid})$ Compute $U_{sid} = (V \oplus h(IID SK N_2))$ Compute $N_2 = (U \oplus h(U_{sid} PW_i SHS_{sid}))$
STEP 3: User can access the service using secure channel.	

شکل ۷: مرحله توافق کلید در پروتکل کومار و چوهان [۱۷]

مرحله تغییر رمز عبور

در پروتکل کومار و چوهان [۱۷]، کاربر خانه هوشمند هنگام تغییر شبکه یا مکان جدید می‌تواند رمز ورود خود را به روز کند. کاربر خانه هوشمند کارت هوشمند را وارد دستگاه کرده و با وارد کردن اطلاعات منحصر به فرد خود، وارد سامانه می‌شود. کارت هوشمند، مقدار $h(IID_u || IID_d)$ را محاسبه می‌کند و از سرور گره خانه می‌خواهد تا رمز عبور خود را با کمک $PC = h(PW_i || IID_u || IID_d || Bio_i)$ به روز کند، اگر مقدار $PC' = PC$ باشد اجازه انجام شدن می‌دهد، در غیر این صورت جلسه را متوقف می‌کند. سپس، سرور خانگی خانه هوشمند اجازه تغییر رمز عبور خود را می‌دهد. در [۱۷] اشاره شده است که پروتکل کومار و چوهان دارای خاصیت گمنامی است و در برابر حمله جعل دستگاه، حمله حدس گذر واژه برون خط، حمله نقض امنیت پیشرو، حمله مرد میانی، حمله تغییر رمز عبور، حمله ردیابی، حمله جعل پیام،

حمله تکرار و حمله به تسخیر در آوردن دستگاه مقاوم است و امنیت این پروتکل به صورت صوری توسط ابزار Avispa و هم چنین با استفاده از مدل RoR نشان داده شده است.

۳-۲ پروتکل پیشنهادی کومارپاندا و چیتاپدهی^۱

در [۱۸] یک پروتکل احراز اصالت امن برای محیط اینترنت اشیاء و سرورهای ابری بر اساس رمزنگاری منحنی بیضوی پیشنهاد شده است. در [۱۸]، ویژگی‌های امنیتی پروتکل پیشنهادی با استفاده از ابزارهای اعتبارسنجی خودکار پروتکل‌های امنیتی به صورت صوری و غیرصوری مورد تجزیه و تحلیل قرار گرفته و با پروتکل‌های مرتبط و مشابه از نظر ویژگی‌های امنیتی مختلف مانند حفظ حریم خصوصی دستگاه، مقاومت در برابر حمله جعل هویت، حمله حدس زدن رمز عبور، برآورده نمودن احراز اصالت متقابل و غیره مقایسه شده است. علاوه بر این، عملکرد پروتکل پیشنهادی از نظر هزینه‌های محاسباتی، ارتباطاتی، سربار ذخیره‌سازی و کل زمان اجرا نیز ارزیابی شده است. تجزیه و تحلیل امنیتی و عملکردی انجام شده در [۱۸] برتری پروتکل کومارپاندا و چیتاپدهی را نسبت به سایر پروتکل‌های مشابه نشان می‌دهد. پروتکل ذکر شده، دارای سه مرحله ثبت‌نام، مرحله ورود و احراز اصالت است. جدول ۳ نمادها و علائم مورد استفاده در پروتکل ذکر شده را نشان می‌دهد.

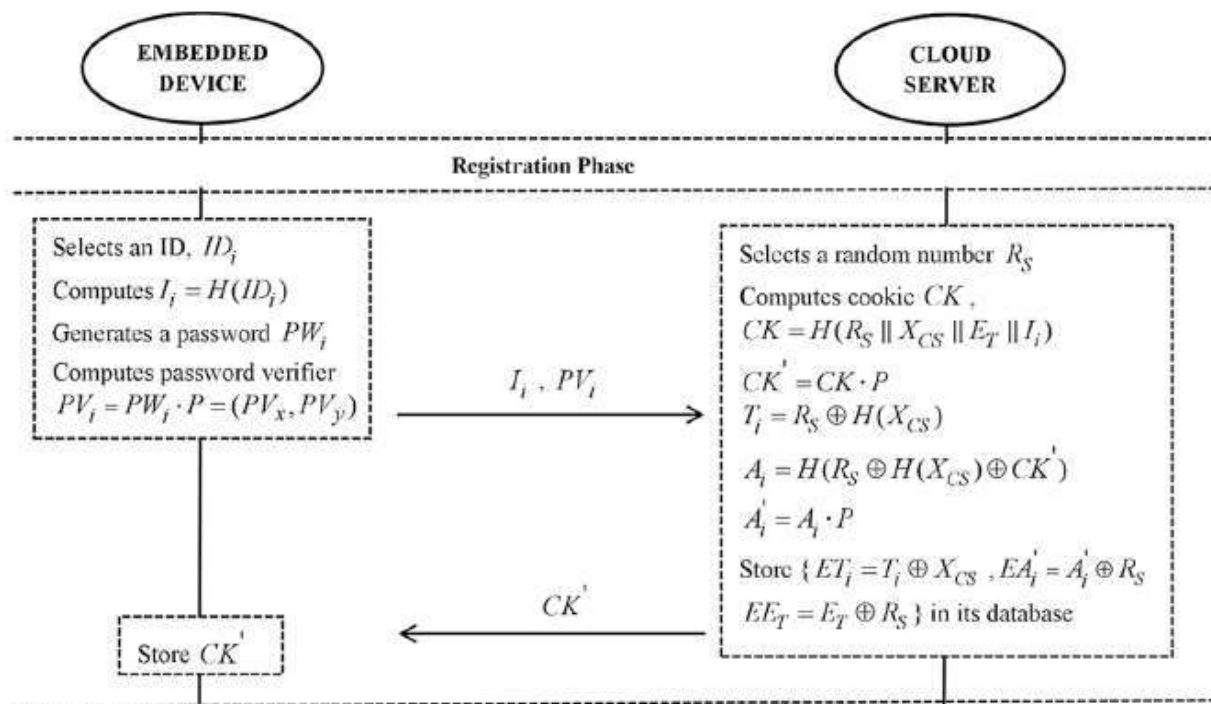
جدول ۳: علائم و نشانه‌های استفاده شده در پروتکل کومارپاندا و چیتاپدهی [۱۸]

Notations	Descriptions
ED_i	An embedded device
CS	The cloud server
ID_i	The identity of the device ED_i
E	An elliptic curve equation
$E_q(a, b)$	An elliptic curve, where a and b are two constant
E_g	An elliptic curve group over E
P	Public point/generator point of the elliptic curve group with order n such that $n \cdot P = 0$
q, n	Large prime numbers
Z_q	A finite field over a large prime number q
PW_i	Password of device ED_i
PV_i	Password verifier of device ED_i , where $PV_i = PW_i \cdot P$
X_{CS}	Server's secret key select from $[1, n - 1]$
R_S	Server's random number
R_1, R_2	Random numbers select from $[1, n - 1]$
$H()$	One-way cryptographic hash function
CK	Cookie information
E_T	Expiration time of the Cookie
SK	Session key individually generated by ED_i and CS

مرحله ثبت‌نام در پروتکل کومارپاندا و چیتاپدهی

شکل ۸ مرحله ثبت‌نام در پروتکل کومارپاندا و چیتاپدهی را نشان می‌دهد.

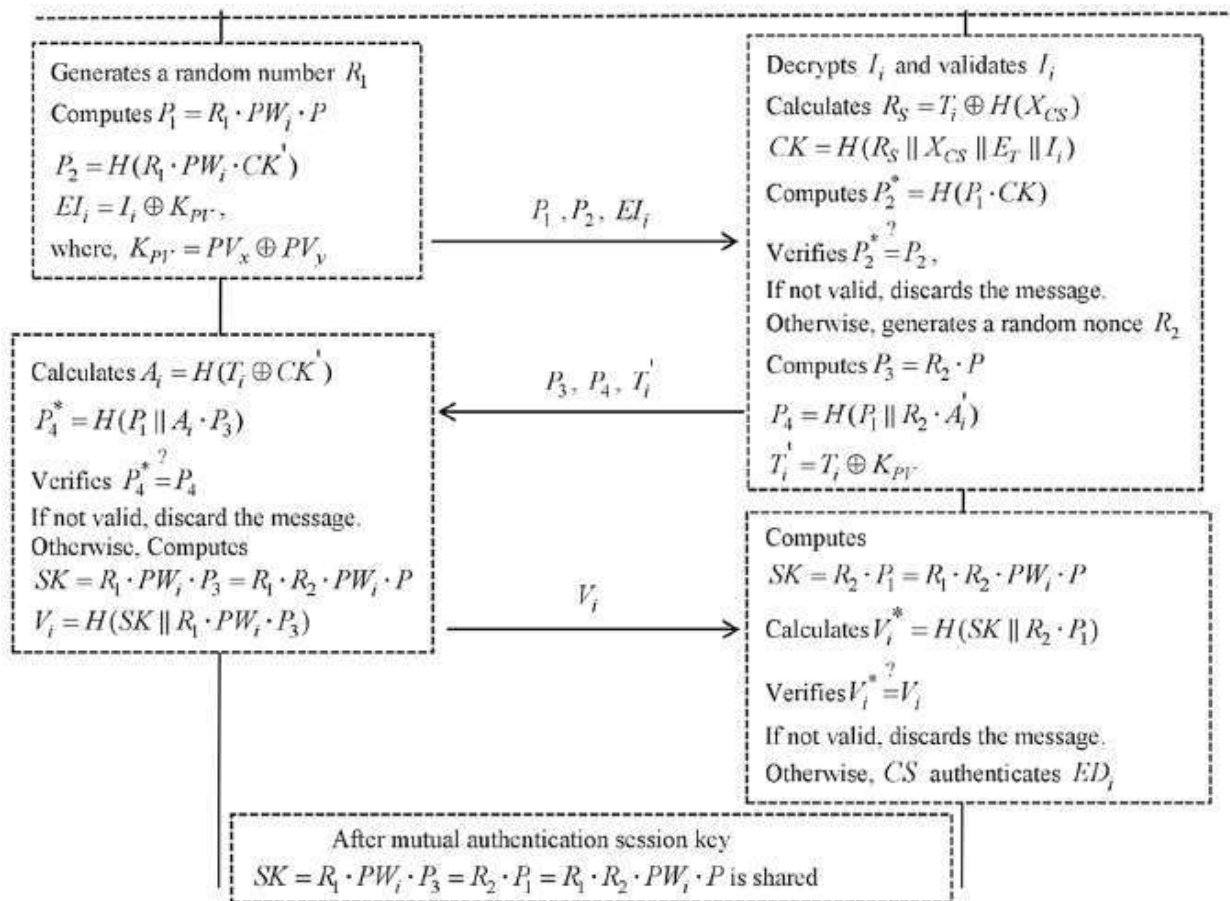
^۱ - Prabhat Kumar Panda, Sudipta Chattopadhyay



شکل ۸: مرحله ثبت نام در پروتکل کومارپاندا و چیتاپدهی [۱۸]

مرحله ورود و احراز اصالت در پروتکل کومارپاندا و چیتاپدهی

شکل ۹ مرحله ورود و احراز اصالت در پروتکل کومارپاندا و چیتاپدهی را نشان می دهد.



شکل ۹: مرحله ورود و احراز اصالت در پروتکل کومار پاندا و چیتاپدهی [۱۸]

در [۱۸] ادعا شده که پروتکل پیشنهادی نویسندگان در برابر حمله منع خدمت، حمله استراق سمع، حمله حدس رمز عبور، حمله جعل هویت، حمله مردمیانی، حمله داخلی الویت دار، حمله تکرار، حمله نقض امنیت پیشرو امن است و نیز دارای خواص احراز اصالت متقابل، حفظ حریم خصوصی دستگاه و کلید توافق جلسه است.

۴-۲ طرح احراز اصالت سونگاتی و همکاران

علائم حیاتی و پارامترهای فیزیولوژیکی بیمار را می توان با گره های حسگر متصل به شبکه حسگر بدن بیمار کنترل کرد و سپس از طریق رسانه های ارتباط بی سیم مانند بلوتوث، WiFi، 3G/4G به پزشک متخصص مربوطه منتقل کرد. در عین حال، امنیت و حریم خصوصی داده های بیمار باید در برابر انواع تهدیدات و آسیب در محیط عمومی و نا امن محافظت شود. در این راستا، در [۱۹] یک طرح احراز اصالت متقابل برای اطمینان از امنیت و حفظ حریم خصوصی بیمار پیشنهاد شده است. طرح احراز اصالت پیشنهادی همچنین از تلفن هوشمند به عنوان یک گره دروازه استفاده می کند که امکان نظارت مستمر بر بیمار را حتی در یک محیط غیربالینی فراهم می کند. علاوه بر این، این طرح شامل یک مرحله برای سناریوی اضطراری است که به موجب آن کیفیت مراقبت از بیمار در شرایط بحرانی حفظ می شود. تحلیل امنیتی انجام شده در [۱۹] نشان می دهد که طرح پیشنهادی در مقایسه با سایر طرح های مرتبط اخیر کارآمدتر است. پروتکل پیشنهادی سونگاتی و

همکاران شامل مراحل زیر است: (۱) ثبت نام، (۲) ورود به سامانه و احراز اصالت، (۳) تغییر رمز عبور و (۴) سناریوی اضطراری. جدول ۴ نمادهای به کار برده شده را در پروتکل سونگاتی و همکاران [۱۹] را نشان می دهد.

جدول ۴: علائم و نشانه های استفاده شده در پروتکل سونگاتی و همکاران [۱۹]

Notation	Description
SN_k	Sensor node $k, k = 1, 2, 3 \dots, n$
ID_{SN_k}	Identity of sensor node $k, k = 1, 2, 3 \dots, n$
ID_U	Identity of patient
PW_U	Password of the patient U
PID_U	Pseudo identity of patient U
ID_D	Identity of doctor D
PW_D	Password of the doctor D
ID_{GW}	Identity of Gateway GW
S	Commitment value computed at the server
x_s	Secret key of the server
x_d	Secret key stored at the doctor's mobile
m_i	32 bit random track sequence number generated by the server for communicating with the patient
d_i	32 bit random track sequence number for communicating with the medical professional
K_{GWS}	Long term secret key shared between the gateway GW and the server S
SK_{GWS}	Shared session key between the gateway GW and the server S
SK_{DS}	Shared session key between the doctor D and the server S
$\oplus$	XOR operation

مرحله ثبت نام کاربر در پروتکل سونگاتی و همکاران

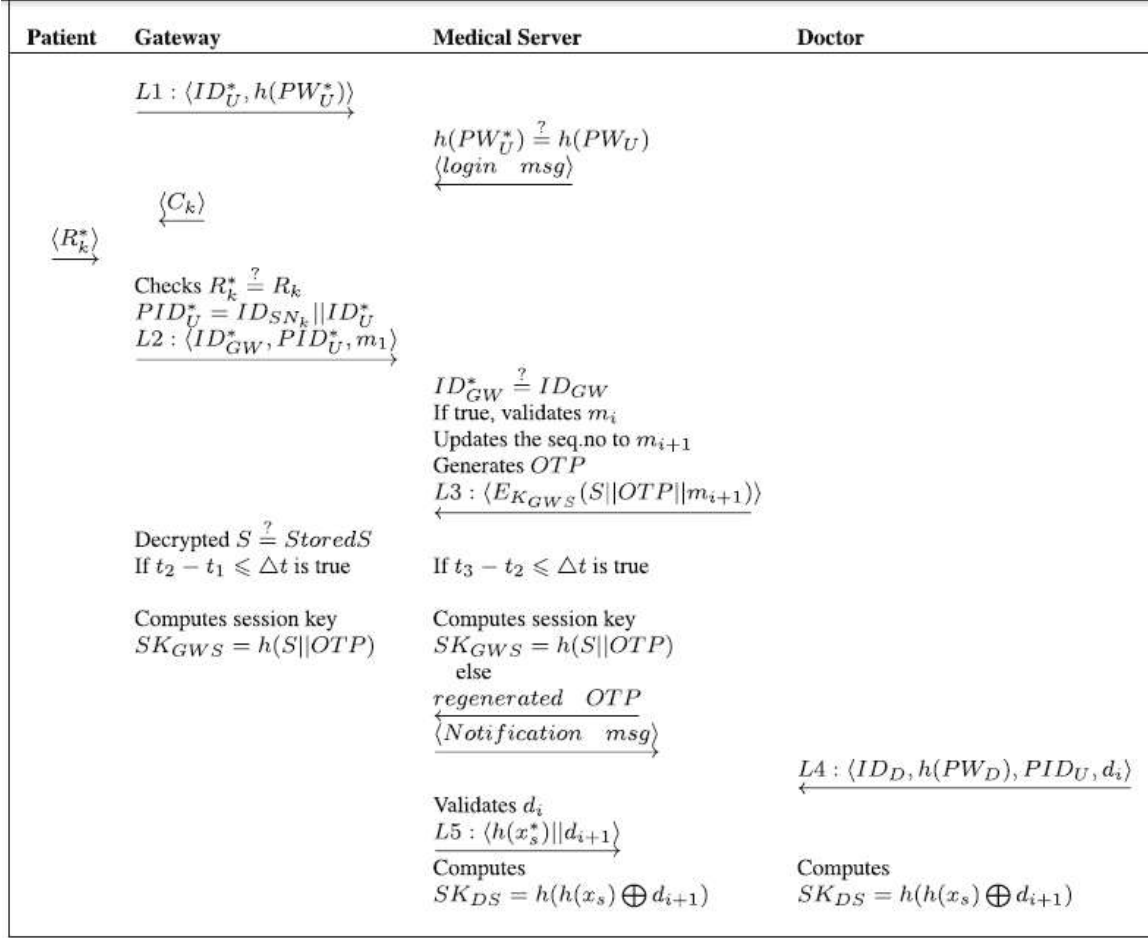
شکل ۱۰ مرحله ثبت نام کاربر را در پروتکل سونگاتی و همکاران را نشان می دهد.

Patient	Medical Server	Doctor/
Patient registers ID_U, PW_U with GW Gateway device generates CRP_k for each $SN_k, k = 1, \dots, n$ $ID_{SN_k} \leftarrow R_k$ Stores $ID_{SN_k}, CRP_k, h(PW_U)$ $PID_U = (ID_{SN_k} ID_U), k = 1, \dots, n$ $\langle ID_U, PID_U, h(PW_U), ID_{GW} \rangle$	$S = h(PID_U ID_{GW} x_s)$ Generates m_1 (Random Seq no) $K_{GWS} = S \oplus h(PW_U)$ Stores $ID_U, PID_U, h(PW_U), ID_{GW}, S, m_1$ $\langle K_{GWS}, m_1 \rangle$	
Stores K_{GWS}, S, m_1	$\langle ID_U, h(x_s), h(x_d), d_i \rangle$ Stores $ID_D, h(PW_D)$ Generates secret key x_d $\langle ID_d, h(x_d) \rangle$	$\langle ID_D, h(PW_D), ID_U \rangle$ Stores $h(x_d), PID_U, h(x_s)$

شکل ۱۰: مرحله ثبت نام در پروتکل سونگاتی و همکاران [۱۹]

مرحله ورود و احراز اصالت در پروتکل سونگاتی و همکاران

مرحله ورود به و احراز اصالت در پروتکل سونگاتی و همکاران [۱۹] در شکل ۱۱ نشان داده شده است.



شکل ۱۱: مرحله ورود و احراز اصالت در پروتکل سونگاتی و همکاران [۱۹]

مرحله تغییر رمز عبور در پروتکل سونگاتی و همکاران

در این طرح هر زمان که بیمار بخواهد رمز عبور PW_U را با رمز ورود جدید یعنی $(pw_U)_{NEW}$ تغییر دهد، مراحل زیر را انجام می‌دهد.

بیمار پس از ورود به سامانه گزینه "تغییر رمز عبور" را انتخاب می‌کند. بیمار رمز جدید PW_U^1 را تایپ می‌کند و دروازه مقدار $h(PW_U^1)$ را محاسبه می‌کند. از بیمار خواسته می‌شود تا رمز عبور را تأیید کند. رمز عبور PW_U^1 گرفته شده و در مقایسه با PW_U^2 به صورت $PW_U^2 = PW_U^1$ مقایسه می‌شود. در این صورت، رمز عبور جدید $(pw_U)_{NEW}$ به عنوان PW_U^2 تنظیم می‌شود. تغییر رمز عبور برای پزشک متخصص نیز به روش فوق تکرار می‌شود در حالی که اعتبار سنجی در سرور انجام می‌شود.

سناریوی اضطراری در پروتکل سونگاتی و همکاران

سرور پزشکی در هنگام ثبت نام، لیست پزشکان، خدمات آمبولانس و شماره تماس آن‌ها را به بیمار ارائه می‌دهد. علاوه بر این، دروازه دامنه معتبری از داده‌ها را برای هر یک از حسگرهای شبکه حسگر بدنی BSN ذخیره می‌کند. هنگامی که بیمار در گره دروازه ثبت نام می‌کند، پارامترها با توجه به سن و وضعیت سلامتی بیمار ثبت می‌شوند. در طرح پیشنهادی [۱۹] دروازه پارامترهای فیزیولوژیکی مانند فشارخون، سطح قندخون و غیره را از حسگرهای مناسب نصب شده

¹-Body Sensor Network

در شبکه حسگر بدن بیمار (BSN) جمع‌آوری می‌کند. برای هر پارامتر، محدوده طبیعی در یک جدول در دستگاه دروازه ثبت می‌شود. به عنوان مثال، فشارخون سالم و ناسالم مطابق با انجمن قلب آمریکا در جدول ۵ آورده شده‌است. اگر میزان فشارخون در محدوده طبیعی یا ۱۲۰/۸۰ میلی متر جیوه باشد، پزشکان اقدامی انجام نمی‌دهند، در همان زمان، هنگامی که فشارخون بیمار در محدوده فشارخون بالا قرارگیرد، پزشک اقدامات مربوط به وضعیت بیمار را انجام می‌دهد. از طرف دیگر، اگر میزان فشارخون به طور ناگهانی از ۱۲۰/۱۸۰ میلی متر جیوه بیشتر شود، ممکن است نشانه‌هایی از آسیب احتمالی اندام مانند درد قفسه سینه، تنگی نفس، کمردرد، بی‌حسی/ضعف، تغییردر بینایی، دشواری درگفتار باشد که نیاز فوری به توصیه‌های پزشکی دارد. از این رو، باید بلافاصله پیام هشدار به پزشک ارسال شود یا خدمات سرپایی انجام شود.

جدول ۵: میزان استاندارد فشار خون [۱۹]

Systolic (mmHg)		Diastolic (mmHg)	Blood pressure category	Response
Less than 120	and	Less than 80	Normal	Null
120–129	and	Less than 80	Elevated	Notification
130–180	or	80–120	High BP and Hypertension	Alert to the doctor
Above 180	and/or	Above 120	Hypertensive crisis	Immediate alert to the doctors and or ambulatory services

در [۱۹] اشاره شده است که پروتکل سونگاتی و همکاران دارای خواص احراز اصالت متقابل و گمنامی و امنیت پیشرو است و در برابر حملاتی مانند افشای کلید نشست، حمله تکرار، حمله حدس برون/درون خط رمزعبور، جعل هویت کاربر، جعل هویت سرور، جعل هویت دروازه و جعل هویت بیمار، حمله به سرقت رفتن دستگاه تلفن همراه مقاوم است. همچنین امنیت این پروتکل به صورت صوری با منطق BAN اثبات شده‌است.

۲-۵ پروتکل مجمودار و همکاران^۱

پروتکل CoAP، یک پروتکل مبتنی بر لایه کاربرد است که یک نسخه فشرده از پروتکل HTTP است که برای ارتباط بین دستگاه‌های منبع محدود در شبکه اینترنت اشیاء IoT استفاده می‌شود. پروتکل CoAP عموماً با UDP مرتبط است و بر اساس معماری انتقال حالت کار می‌کند. CoAP با پروتکل DTLS برای ایجاد یک جلسه امن با استفاده از الگوریتم‌های موجود برای ارتباط بین دستگاه‌های مختلف اینترنت اشیا و سرور از راه دور در ارتباط است. با این حال، چندین محدودیت در مورد مدیریت کلید، ایجاد جلسه و ارتباط پیام‌های چندرسانه‌ای در لایه DTLS در CoAP وجود دارد. برای غلبه بر محدودیت‌های موجود مربوط به مدیریت کلید و امنیت چندرسانه‌ای در CoAP، در [۲۰] یک طرح ارتباطی کارآمد و ایمن برای ایجاد کلید جلسه امن بین دستگاه‌های IoT و سرور از راه دور با استفاده از رمزنگاری منحنی بیضوی سبک وزن (ECC) پیشنهاد شده است. پروتکل CoAP پیشنهادی مبتنی بر ECC به عنوان ECC-CoAP نامیده می‌شود که پیاده‌سازی CoAP را برای احراز اصالت در شبکه اینترنت اشیا نشان می‌دهد. تعدادی از حملات رمزنگاری معروف برای تأیید قدرت امنیتی ECC-CoAP مورد تجزیه و تحلیل قرار گرفته و مشخص شده است که در مقابل این حملات به خوبی مقاوم است. تجزیه و تحلیل عملکرد ECC-CoAP نشان می‌دهد که طرح پیشنهادی [۲۰] سبک و ایمن است. طرح پیشنهادی [۲۰] شامل چند مرحله است که شامل: شروع جلسه، مرحله چالش سرور، پاسخ کاربر،

^۱-Majumder et al.

^۲-Constraint Application Protocol

^۳-User datagram protocol

^۴-Datagram transport layer security

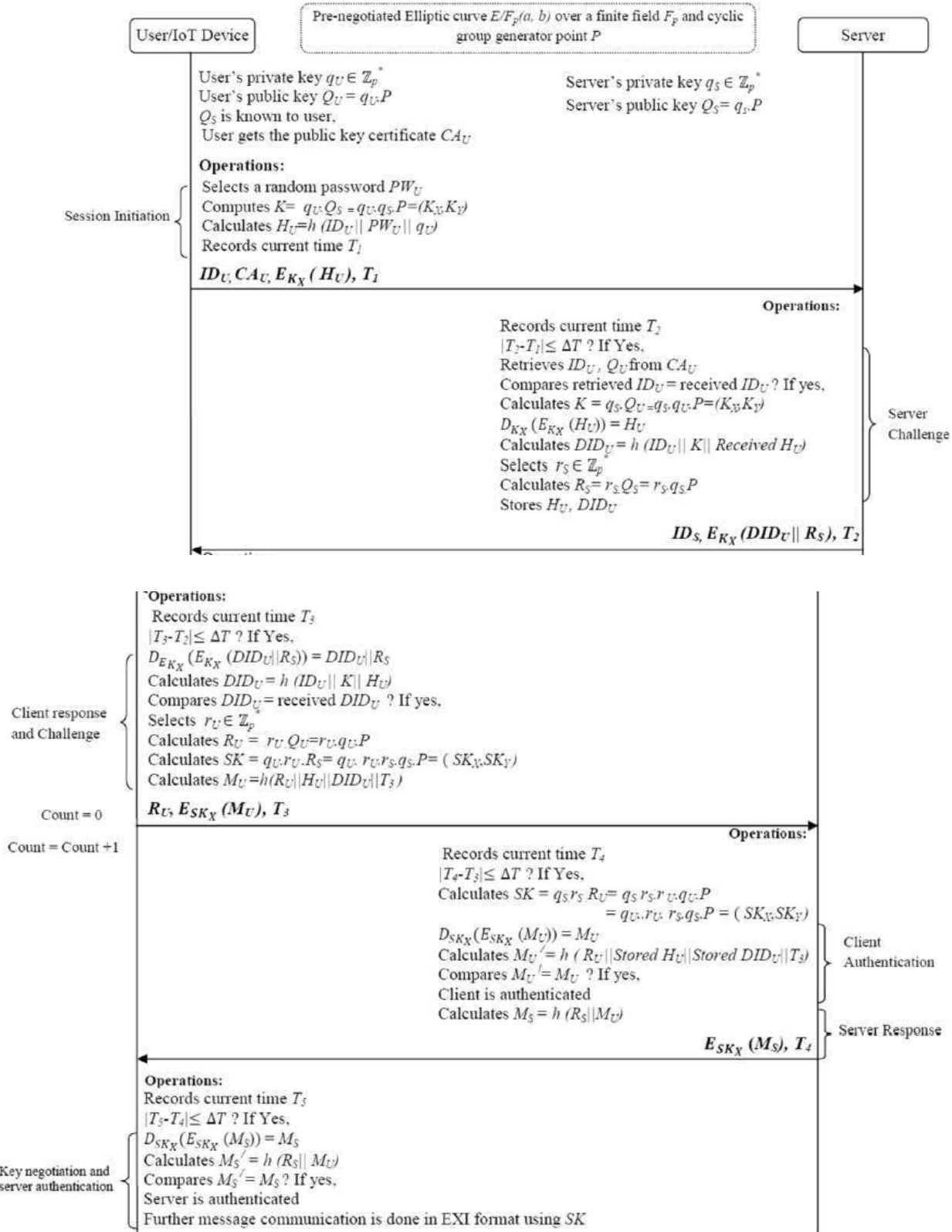
^۵-Elliptic Curve Cryptography Based Constraint Application Protocol

مرحله چالش احراز اصالت کاربر، مرحله پاسخ سرور و مرحله مذاکره کلید و احراز اصالت سرور است. جدول ۶ نمادهای به کار برده شده در پروتکل مجمودار و همکاران را نشان می‌دهد.

جدول ۶: نمادها و علائم مورد استفاده در پروتکل مجمودار و همکاران [۲۰]

Notation	Description
U	User/IoT device
S	Server
F_p	A large prime finite field over p
$E_p(a,b)$	An elliptic curve is defined on F_p
P	A generator point on $E/F_p(a,b)$ with order n
ID_U	User's identity
PW_U	Random password selected by the user
DID_U	Dynamic login identity of the user/device generated by server
K	Common key used for Encryption/Decryption for both user/IoT device and server end
S_K	Dynamic session identity generated from server end
r_U	Random number selected by the user
r_S	Random number selected by the server
R_U	Random value produced by the user where $R_U = r_U \cdot Q_U$
R_S	Random value produced by the server where $R_S = r_S \cdot Q_S$
$h(.)$	One way secure hash function such as <i>SHA1</i>
E/D	Symmetric encryption/decryption algorithm
(q_S, Q_S)	Private-public key pair of server where $Q_S = q_S \cdot P$
(q_U, Q_U)	Private-public key pair of user/IoT device where $Q_U = q_U \cdot P$
$ $	Concatenation

مراحل مختلف پروتکل مجمودار و همکاران [۲۰] در شکل ۱۲ نشان داده شده است. مراحل پروتکل مجمودار و همکاران به این صورت است که ابتدا جلسه شروع می‌شود. سپس سرور در پاسخ به کاربر یا دستگاه اینترنت اشیا یک روال محاسباتی را طی می‌کند که از آن با عنوان چالش سرور یاد می‌شود. سرور در پاسخ به کاربر اطلاعاتی را برای کاربر یا دستگاه اینترنت ارسال می‌کند و یک چالش و پاسخ در سمت کاربر شروع می‌شود. سپس در نهایت با انجام روال ارسال از سمت فرستنده به سرور احراز اصالت رخ می‌دهد و در نهایت یک توافق کلید و احراز اصالت بین فرستنده و گیرنده رخ می‌دهد. در [۲۰] بیان شده است که پروتکل مجمودار و همکاران دارای خاصیت احراز اصالت متقابل است و در برابر حملاتی مانند حمله مردمیانی، حمله منع خدمت، حمله تکرار، حمله داخلی، حمله جعل هویت کاربر، حمله جعل هویت سرور، حمله حدس رمز عبور برون خط، حمله محاسبه کلید نشست و حمله نقض امنیت پیشرو مقاوم است.



شکل ۱۲: مرحله ثبت نام و احراز اصالت در پروتکل مجمودار و همکاران [۲۰]

۲-۶ طرح احراز اصالت کال و آوستی

کال و آوستی در [۲۱] یک پروتکل احراز اصالت مناسب محیط‌های دارای محدودیت منابع را ارائه کرده‌اند. آنها ادعا کردند که پروتکل معرفی شده آنها برای کاربردهای دنیای واقعی کارآمد و ایمن است. بعد از آن رانا و همکاران در [۲۲] نشان دادند که پروتکل کال و آوستی ایمن نیست زیرا مهاجم می‌تواند به راحتی هویت یک کاربر قانونی را که در کانال عمومی ارسال می‌شود را بیابد. علاوه بر این، با استفاده از هویت یک کاربر مجاز، مهاجم می‌تواند خود را به عنوان یک کاربر مجاز معرفی کند و از خدمات ارائه شده توسط سرور بهره ببرد. بنابراین، پروتکل کال و آوستی مستعد حملات جعل هویت کاربر است. رانا و همکاران در [۲۲] پروتکل کال و آوستی را اصلاح کرده و با اطمینان از ارتباط ایمن در کل کانال، طرح ارتقا یافته‌ای را ارائه کرده‌اند. علاوه بر این، رانا و همکاران ادعا کرده‌اند که پروتکل پیشنهادی آنها نه تنها در برابر حملات جعل هویت کاربر بلکه دیگر حملات امنیتی نیز ایمن است و کاندیدای بهتری برای استقرار در شبکه‌های 6G/IoT است. پروتکل کال و آوستی شامل چهار مرحله ثبت‌نام، ورود و احراز اصالت و تغییر رمز عبور است. لازم به ذکر است، که علائم و نمادهای مورد استفاده در پروتکل کال و آوستی در جدول ۷ نشان داده شده است.

جدول ۷: نمادها و علائم مورد استفاده در پروتکل کال و آوستی [۲۱]

U_i	Legitimate i th user
ID_i	Identifier of U_i
PW_i	Password of U_i
S	Server
x, y	Secret key and number of the server S
y_i	Unique random number for i th user assigned by S
SK	Session key
SC_i	i th user smart card
T	Current time stamp of input device
T_s	Current time stamp of server
δT	Expected time interval for a transmission delay
$h(.)$	Secure one way hash function $h(.) : \{0, 1\}^* \rightarrow \{0, 1\}^{128}$
$\oplus$	Bitwise XOR operation
$\parallel$	Concatenation operation

مرحله ثبت‌نام، ورود و احراز اصالت در پروتکل کال و آوستی

مراحل ثبت‌نام، ورود، احراز اصالت و تغییر رمز عبور در پروتکل کال و آوستی به ترتیب در شکل‌های ۱۳، ۱۴، ۱۵ و ۱۶ نمایش داده شده است.

User	Server (x, y)
Choose ID_i and PW_i	
Choose random number b	
Compute $RPW_i = h(b \ PW_i)$	
$ID_i, RPW_i \longrightarrow$	
	Choose unique random number y_i
	Compute $\alpha_i = h((ID_i \oplus x) \ y)$
	$\beta_i = \alpha_i \oplus h(ID_i \oplus RPW_i)$
	$\gamma_i = y_i \oplus h(\alpha_i \oplus RPW_i)$
	$\chi_i = h(ID_i \ RPW_i \ y_i \ \alpha_i)$
	Store $\{\beta_i, \gamma_i, \chi_i, h(\cdot)\}$ on smart card
	$SmartCard \longleftarrow$
Compute $\eta_i = b \oplus h(ID_i \oplus PW_i)$	
Store $\{\eta_i\}$ on smart card	

شکل ۱۳: مرحله ثبت نام در پروتکل کال و آوستی [۲۱]

User	Smart card	Server
Input ID_i^* and PW_i^*		
	Compute $b = \eta_i \oplus h(ID_i^* \oplus PW_i^*)$	
	$RPW_i^* = h(b \ PW_i^*)$	
	$\alpha_i^* = \beta_i \oplus h(ID_i^* \oplus RPW_i^*)$	
	$y_i^* = \gamma_i \oplus h(\alpha_i^* \oplus RPW_i^*)$	
	$\chi_i^* = h(ID_i^* \ RPW_i^* \ y_i^* \ \alpha_i^*)$	
	Verify $\chi_i^* \stackrel{?}{=} \chi_i$	
	Compute $\omega_i = y_i \oplus h(ID_i \oplus \alpha_i) \oplus h(ID_i \oplus \alpha_i \oplus T)$	
	$\vartheta_i = h(ID_i \ \alpha_i \ y_i \ (\alpha_i \oplus y_i) \ T)$	
	$ID_i, \omega_i, \vartheta_i, T \longrightarrow$	

شکل ۱۴: مرحله ورود در پروتکل کال و آوستی [۲۱]

Smart card	Server
$ID, \omega_i, \vartheta_i, T \longrightarrow$	
Verify $(T' - T) \leq \delta T$ Compute $\alpha_i^* = h((ID_i^* \oplus x) \ y)$ $y_i^* = \omega_i^* \oplus h(ID_i^* \oplus \alpha_i^*) \oplus h(ID_i^* \oplus \alpha_i^* \oplus T)$ $\vartheta_i^* = h(ID_i^* \ \alpha_i^* \ y_i^* \ (\alpha_i^* \oplus y_i^*) \ T)$ Verify $\vartheta_i^* \stackrel{?}{=} \vartheta_i$ Compute $\mu_i = h(ID_i \ y_i \ (\alpha_i \oplus y_i) \ T_s)$ $\mu_i, T_s \longleftarrow$	
Verify $(T'_s - T_s) \leq \delta T_s$ Compute $\mu_i^* = h(ID_i \ y_i \ (\alpha_i \oplus y_i) \ T_s)$ Verify $\mu_i^* \stackrel{?}{=} \mu_i$ Generate session key $SK = h(ID_i \oplus \alpha_i \oplus y_i \oplus T \oplus T_s)$	

شکل ۱۵: مرحله احراز اصالت در پروتکل کال و آوستی [۲۱]

User	Smart card
Input ID_i^*, PW_i^* and PW_i^N	
Compute $b = \eta_i \oplus h(ID_i^* \oplus PW_i^*)$ $RPW_i^* = h(b \ PW_i^*)$ $\alpha_i^* = \beta_i \oplus h(ID_i^* \oplus RPW_i^*)$ $y_i^* = \gamma_i \oplus h(\alpha_i^* \oplus RPW_i^*)$ $\chi_i^* = h(ID_i^* \ RPW_i^* \ y_i^* \ \alpha_i^*)$ Verify $\chi_i^* \stackrel{?}{=} \chi_i$ Compute $RPW_i^N = h(b \ PW_i^N)$ $\beta_i^N = \alpha_i \oplus h(ID_i \oplus RPW_i^N)$ $\gamma_i^N = y_i \oplus h(\alpha_i \oplus RPW_i^N)$ $\chi_i^N = h(ID_i \ RPW_i^N \ y_i \ \alpha_i)$ $\eta_i^N = b \oplus h(ID_i \oplus PW_i^N)$ Update $\beta_i^N, \gamma_i^N, \chi_i^N, \eta_i^N$ on smart card	

شکل ۱۶: مرحله تغییر رمز عبور در پروتکل کال و آوستی [۲۱]

همان طور که اشاره شد، پروتکل کال و آوستی در برابر حمله جعل مقاوم نیست، از این رو رانا و همکاران در [۲۲] پروتکل بهبود یافته طرح آنها را ارائه دادند. در پروتکل رانا و همکاران ادعا شده است که در برابر طیف وسیعی از حملات مقاوم است.

حمله جعل بر علیه پروتکل کال و آوستی

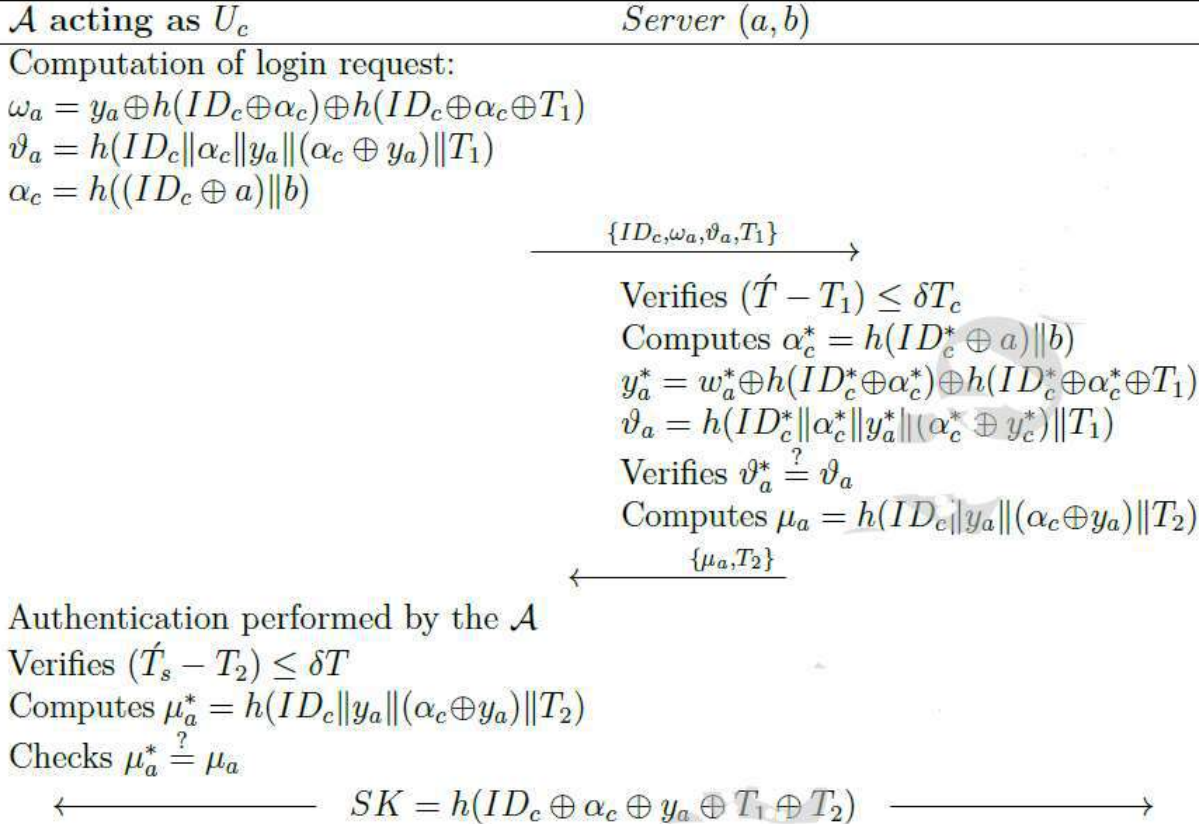
مهاجم درخواست احراز اصالت یک کاربر را شنود می کند $\{ID_c, W_c, V_c, T_1\}$ تا اطلاعات آن نظیر $\{ID_c, U_c\}$ را به دست آورد. سپس با انتخاب یک رمز عبور PW_a و یک مقدار دلخواه مثل m_a مقدار RPW_a را به صورت $RPW_a = h(m_a \parallel PW_a)$ محاسبه می کند و سپس درخواست ثبت نام $\{RPW_a, ID_c\}$ را برای سرور ارسال می کند. سرور با دریافت اطلاعات فوق، مقادیر زیر را محاسبه می کند:

$$\begin{aligned} a_c &= h((ID_c \oplus a) \parallel b) \\ B_a &= a_c \oplus h(ID_c \oplus RPW_a) \\ Y_a &= y_a \oplus h(a_c \oplus RPW_a) \\ X_a &= h(ID_c \parallel RPW_a \parallel y_a \parallel a_c) \end{aligned}$$

سپس سرور اطلاعات $\{X_a, B_a, Y_a, h(\cdot)\}$ را در کارت هوشمند ذخیره می کند و برای مهاجم ارسال می کند. مهاجم بعد از دریافت اطلاعات فوق، مقادیر $\{X_a, B_a, Y_a, h(\cdot)\}$ را استخراج می کند و سپس مقادیر a_c, y_a را به صورت زیر بازیابی می کند.

$$\begin{aligned} a_c &= B_a \oplus h(ID_c \oplus RPW_a) \\ y_a &= Y_a \oplus h(a_c \oplus RPW_a) \end{aligned}$$

که در آن $RPW_a = h(m_a \parallel PW_a)$ است. بدین صورت با داشتن a_c و y_a یک مهاجم می تواند هویت یک کاربر را جعل کند. لازم به ذکر است که شکل ۱۷ نمایی از حمله جعل وارده بر پروتکل کال و آوستی را نشان می دهد.



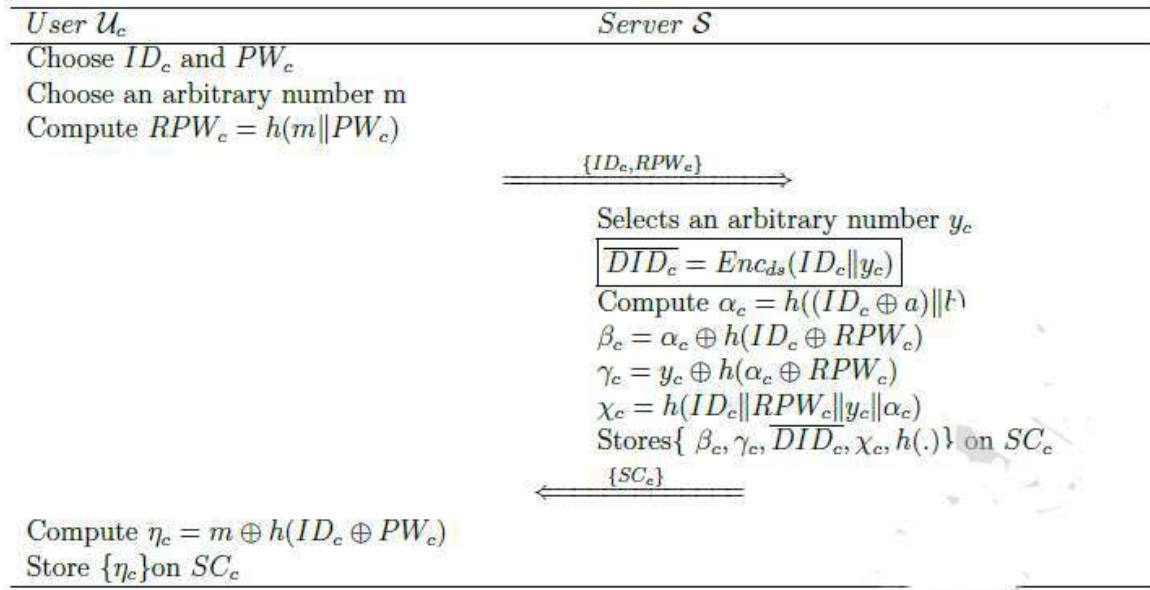
شکل ۱۷: حمله جعل هویت بر علیه پروتکل کال و آوستی [۲۲]

۷-۲ طرح احراز اصالت رانا و همکاران

برای حذف موارد ضعف امنیتی پروتکل کال و آوستی، رانا و همکاران در [۲۲] یک پروتکل احراز اصالت کاربر از راه دور با توافق کلید را ارائه نموده‌اند که تمام ویژگی‌های اساسی طرح کال و آوستی را حفظ می‌کند. علاوه بر این، طرح ارائه شده در [۲۲] تمام مشکلات امنیتی طرح احراز اصالت کال و آوستی را برطرف می‌کند تا پروتکل را برای کاربردهای دنیای واقعی، ایمن و موثر کند. مشابه پروتکل کال و آوستی طرح ارائه شده رانا و همکاران شامل چهار مرحله است: مرحله ثبت‌نام، مرحله ورود به سامانه، مرحله احراز اصالت و مرحله تغییر رمز عبور.

مرحله ثبت نام در طرح احراز اصالت رانا و همکاران

شکل ۱۸ مرحله ثبت‌نام در طرح احراز اصالت رانا و همکاران را نشان می‌دهد.



شکل ۱۸: مرحله ثبت‌نام در طرح احراز اصالت رانا و همکاران [۲۲]

مرحله ورود و احراز اصالت در طرح احراز اصالت رانا و همکاران

شکل ۱۹ مرحله ورود و احراز اصالت را در پروتکل رانا و همکاران را نشان می‌دهد.

مرحله تغییر رمز عبور در طرح احراز اصالت رانا و همکاران

کاربر اطلاعات خود را که نظیر ID_c, PW_c, PW_c^n است را وارد می‌کند.

کارت خوان هوشمند مقدار m را استخراج می‌کند و سپس مقدار RPW_c^* را محاسبه می‌کند.

$$m = \eta_c \oplus h(ID_c^* \oplus PW_c^*)$$

پس از آن، کارت خوان هوشمند مقادیر زیر را استخراج می‌کند.

$$a_c^* = B_c \oplus h(ID_c^* \oplus RPW_c^*)$$

$$y_c^* = Y_c \oplus h(a_c^* \oplus RPW_c^*)$$

سپس، مقدار X_c^* را به صورت $X_c^* = h(ID_c^* || RPW_c^* || y_c^* || a_c^*)$ محاسبه می‌کند. با توجه به مقدار ذخیره شده X_c با مقدار

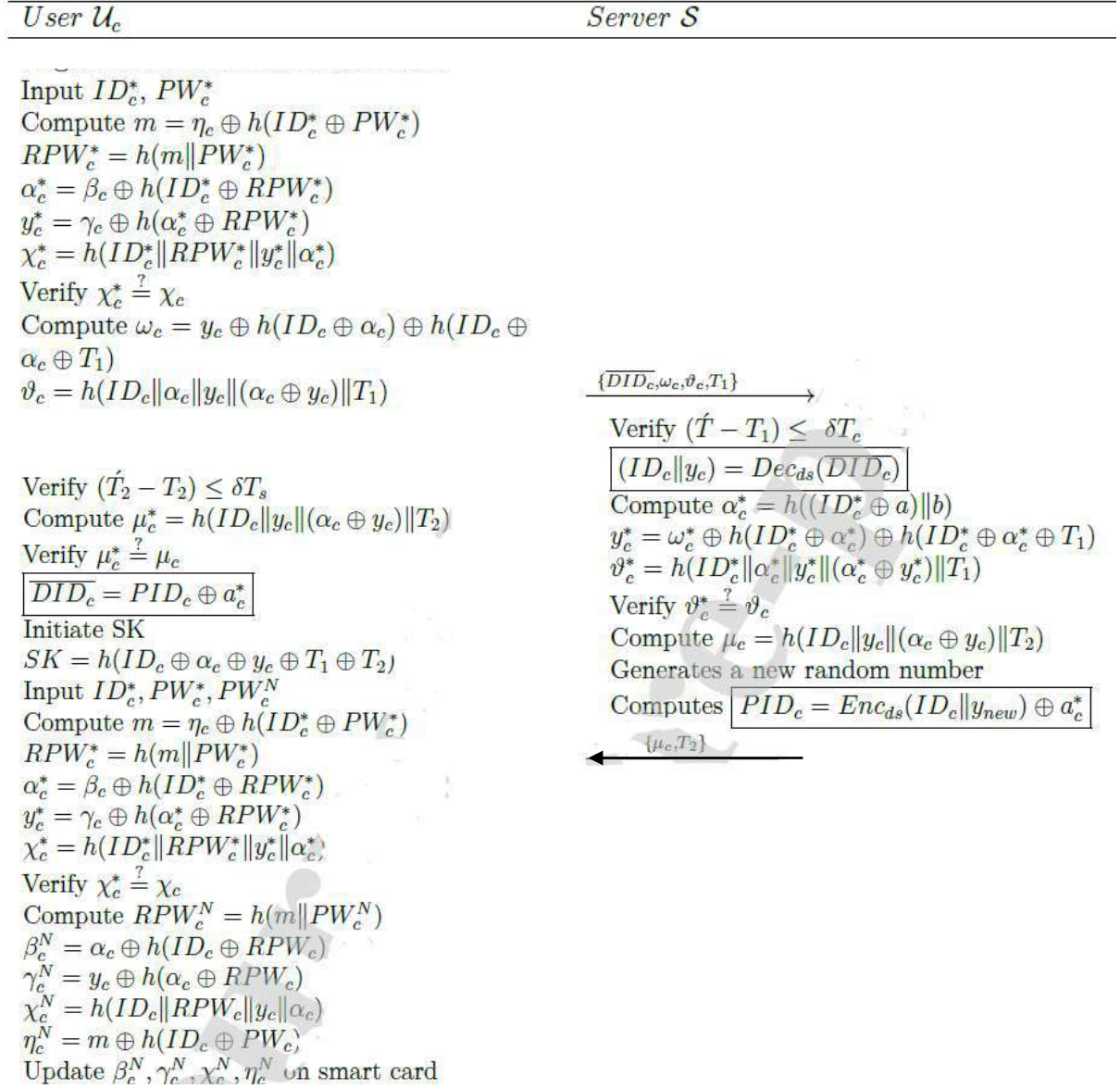
محاسبه شده X_c^* یک مقایسه بین این دو صورت می‌گیرد، اگر این دو مقدار برابر باشند، کاربر می‌تواند رمز عبور خود را

عوض کند. برای کاربر مشروع یا قانونی بعد از عملیات فوق مقادیر زیر محاسبه خواهد شد.

$$RPW_c^N = h(m || PW_c^N)$$

$$\begin{aligned}
B_c^N &= a_c \oplus h(ID_c \oplus RPW_c) \\
Y_c^N &= y_c \oplus h(a_c \oplus RPW_c) \\
X_c^N &= h(ID_c || RPW_c || y_c || a_c) \\
\eta_c &= m \oplus h(ID_c \oplus PW_c)
\end{aligned}$$

در نهایت مقادیر $\{B_c, Y_c, X_c, \eta_c\}$ با مقادیر $\{B_c^N, Y_c^N, X_c^N, \eta_c^N\}$ به روز می شود.



شکل ۱۹: مرحله ورود و احراز اصالت در پروتکل رانا و همکاران [۲۲]

در [۲۲] ادعا شده است که پروتکل پیشنهادی آنها دارای خاصیت احراز اصالت متقابل است و در برابر حمله داخلی الویت دار، به سرقت رفتن کارت هوشمند، حمله جعل کاربر و سرور، حمله حدس رمز عبور/برخط/برون خط، حمله تکرار، حمله منع خدمت و حمله مرد میانی مقاوم است

همان طور که مشاهده شد، برای محیط‌های با محدودیت منابع تاکنون طرح‌های امنیتی بسیاری ارائه شده است که برای بیشتر آنها هم انواع تحلیل‌های امنیتی و حملات مختلف ارائه شده است. این موضوع نشان می‌دهد که هنوز نیاز به پروتکل امن در این حوزه وجود دارد و تاکنون پروتکلی که امن و کارا باشد و با قابلیت‌های محدود این محیط‌ها هم سازگار باشد ارائه نشده است. جدول ۸ خلاصه‌ای از آسیب‌پذیری‌های طرح‌های احراز اصالت پیشنهاد شده برای محیط‌های منبع محدود را نشان می‌دهد.

جدول ۸: خلاصه‌ای از طرح‌های احراز اصالت ارائه شده برای محیط‌های با محدودیت منابع و آسیب‌پذیری‌های آنها و نیز طرح بهبودیافته آن‌ها در صورت وجود

سال	طرح احراز اصالت	ضعف امنیتی	طرح احراز اصالت بهبود یافته	سال
۲۰۲۰	وینود و همکارانش [۱۵]	حمله رله و حمله جعل برچسب	صفخانی و همکارانش [۱۶]	۲۰۲۱
۲۰۲۱	صفخانی و همکاران [۱۶]	-	-	-
۲۰۲۱	کومار و چوهان [۱۷]	-	-	-
۲۰۲۰	کوماریاندا و چیتاپدهی [۱۸]	-	-	-
۲۰۱۹	سونگانی و همکاران [۱۹]	-	-	-
۲۰۲۱	مجمودر و همکاران [۲۰]	-	-	-
۲۰۱۶	کال و آوستی [۲۱]	حمله جعل هویت	طرح رانا و همکاران [۲۲]	۲۰۲۱
۲۰۲۱	رانا و همکاران [۲۲]	-	-	-
۲۰۱۹	شورسکومار و همکاران [۱]	حمله نقض یکپارچگی، عدم ردیابی و غیر همزمان سازی	ECCbAS [۱۴]	۲۰۲۳

۳- دلایل انجام طرح:

یکی از اهداف این پیشنهاد پروژه، شناخت بهتر تهدیدهای امنیتی و عوامل اصلی به وقوع پیوستن آنها در محیط‌های با محدودیت منابع است. برای این محیط‌ها که از لحاظ قابلیت‌های محاسباتی، پردازشی، ذخیره‌سازی و ارتباطی در محدودیت هستند، انواع طرح‌های احراز اصالت ارائه شده است. تشخیص آسیب‌پذیری‌های موجود در این طرح‌های احراز اصالت و بهبود آنها با ویژگی‌های مناسب و قوی امنیتی در این پروتکل‌های امنیتی بسیار حائز اهمیت است. بدیهی است که با مرتفع شدن این مشکلات امنیتی، امنیت این طرح‌های احراز اصالت در برابر طیف مختلفی از حملات بیشتر می‌شود که در نهایت محیط‌های منبع محدود می‌توانند با اطمینان خاطر نسبت به ارائه خدمات از راه دور اقدام نمایند.

۴- اهداف و محصولات طرح:

اهدافی که از انجام این طرح به دست خواهند آمد به شرح زیر است:

- ۱- تحلیل امنیتی و در نهایت افزایش امنیت طرح‌های احراز اصالتی که در انواع محیط‌های با محدودیت منابع مانند شبکه‌های حسگر بی‌سیم، شبکه‌های بی‌سیم بدنی، شهرهای هوشمند و غیره ارائه شده‌اند.
- ۲- ارائه پروتکل‌های احراز اصالت امن متناسب با قابلیت‌های پردازشی، ارتباطی، محاسباتی و ذخیره‌سازی محدود این محیط‌ها

¹-Relay attack

²-Majumder et al.

۵- برنامه و نحوه اجرای طرح:

در راستای اهداف بیان شده در قسمت قبل، اقدامات زیر در جهت تحلیل امنیتی طرح‌های احراز اصالت موجود ارائه شده برای محیط‌های با محدودیت منابع و بهبود امنیت آنها انجام خواهد شد.

- بررسی پیشینه تحقیق
- تحلیل امنیتی پروتکل‌های احراز اصالت ارائه شده برای محیط‌های با محدودیت منابع با استفاده از روش‌های غیرصوری و منطق‌های ریاضی مانند BAN ، GNY و مدل (RoR) Real or Random Model
- تحلیل امنیتی پروتکل‌های احراز اصالت ارائه شده برای محیط‌های با محدودیت منابع با استفاده از نرم‌افزارهای تحلیل امنیتی خودکار مانند AVISPA، Scyther، Proverif و TAMARIN
- مقاوم نمودن پروتکل‌های احراز اصالت آسیب‌پذیر در برابر حملات و بررسی امنیت نسخه‌های بهبود یافته با استفاده از انواع روش‌های صوری، غیرصوری و انواع نرم‌افزارهای خودکار تحلیل امنیتی
- مستند سازی نتایج بدست آمده و انتشار مقاله

۶- برنامه زمانی:

شماره مرحله / فعالیت	نام مرحله / فعالیت	مرحله / فعالیت پیش‌نیاز	درصد وزنی به کل پروژه	مدت زمان اجرا (ماه)	نمودار زمان‌بندی (ماه)											
					۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
۱	بررسی پیشینه تحقیق		۵٪	۱												
۲	تحلیل امنیتی پروتکل‌های احراز اصالت ارائه شده برای محیط‌های با محدودیت منابع با استفاده از روش‌های غیرصوری و منطق‌های ریاضی مانند BAN ، GNY و مدل (RoR) Real or Random Model	۱	۱۵٪	۲												
۳	تحلیل امنیتی پروتکل‌های احراز اصالت ارائه شده برای محیط‌های با محدودیت منابع با استفاده از نرم‌افزارهای تحلیل امنیتی خودکار مانند AVISPA، Scyther، Proverif و TAMARIN	۲ و ۱	۲۰٪	۲												
۴	مقاوم نمودن پروتکل‌های احراز اصالت آسیب‌پذیر در برابر حملات و بررسی امنیت نسخه‌های بهبود یافته با استفاده از انواع روش‌های صوری، غیرصوری و انواع نرم‌افزارهای خودکار تحلیل امنیتی	۳-۲	۳۰٪	۲												

- [5] Shi, X., J. Cao, T. Lu, and V. Chang. *A Survey on RFID Security and Privacy in Smart Medical: Threats and Protections*. in *IoT BDS*. 2019.
- [6] Masdari, M. and S. Ahmadzadeh, *A survey and taxonomy of the authentication schemes in Telecare Medicine Information Systems*. *Journal of Network and Computer Applications*, 2017. **87**: p. 1-19.
- [7] Mishra, S.S. and A. Rasool. *IoT Health care Monitoring and Tracking: A Survey*. in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. 2019. IEEE.
- [8] Alzahrani, B.A. and A. Irshad, *A secure and efficient TMIS-based authentication scheme improved against Zhang et al.'s scheme*. *Arabian Journal for Science and Engineering*, 2018. **43**(12): p. 8239-8253.
- [9] Blanchet, B. and A. Chaudhuri. *Automated formal analysis of a protocol for secure file sharing on untrusted storage*. in *2008 IEEE Symposium on Security and Privacy (sp 2008)*. 2008. IEEE.
- [10] Cremers, C. J. (2008). The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols: Tool Paper. In *Computer Aided Verification: 20th International Conference, CAV 2008 Princeton, NJ, USA, July 7-14, 2008 Proceedings 20* (pp. 414-418). Springer Berlin Heidelberg.
- [11] Zhu, F. (2020). SecMAP: a secure RFID mutual authentication protocol for healthcare systems. *IEEE Access*, 8, 192192-192205.
- [12] Servati, M. R., & Safkhani, M. (2023). ECCbAS: An ECC based authentication scheme for healthcare IoT systems. *Pervasive and Mobile Computing*, 90, 101753.
- [13] Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2017). Authentication protocols for internet of things: a comprehensive survey. *Security and Communication Networks*, 2017.
- [14] Servati, M. R., & Safkhani, M. (2023). ECCbAS: An ECC based authentication scheme for healthcare IoT systems. *Pervasive and Mobile Computing*, 90, 101753.
- [15] Kumar, V., Ahmad, M., Mishra, D., Kumari, S., & Khan, M. K. (2020). RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing. *Vehicular Communications*, 22, 100213.
- [16] Safkhani, M., Camara, C., Peris-Lopez, P., & Bagheri, N. (2021). RSEAP2: An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud computing. *Vehicular Communications*, 28, 100311.
- [17] Kumar, P., & Chouhan, L. (2021). A secure authentication scheme for IoT application in smart home. *Peer-to-Peer Networking and Applications*, 14, 420-438.
- [18] Panda, P. K., & Chattopadhyay, S. (2020). A secure mutual authentication protocol for IoT environment. *Journal of Reliable Intelligent Environments*, 6, 79-94.
- [19] Suganthi, S. D., Anitha, R. V. S. S., Sureshkumar, V., Harish, S., & Agalya, S. (2020). End to end light weight mutual authentication scheme in IoT-based healthcare environment. *Journal of Reliable Intelligent Environments*, 6, 3-13.
- [20] Majumder, S., Ray, S., Sadhukhan, D., Khan, M. K., & Dasgupta, M. (2021). ECC-CoAP: Elliptic curve cryptography based constraint application protocol for internet of things. *Wireless Personal Communications*, 116, 1867-1896.

- [21] Kaul, S. D., & Awasthi, A. K. (2016). Security enhancement of an improved remote user authentication scheme with key agreement. *Wireless Personal Communications*, 89, 621-637.
- [22] Rana, M., Shafiq, A., Altaf, I., Alazab, M., Mahmood, K., Chaudhry, S. A., & Zikria, Y. B. (2021). A secure and lightweight authentication scheme for next generation IoT infrastructure. *Computer Communications*, 165, 85-96.
- [23] Burrows, M., M. Abadi, and R.M. Needham, *A logic of authentication*. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 1989. **426**(1871): p. 233-271.
- [24] Gong, L., R.M. Needham, and R. Yahalom. *Reasoning about Belief in Cryptographic Protocols*. in *IEEE Symposium on Security and Privacy*. 1990. Citeseer.
- [25] Armando, A., D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P.H. Drielsma, P.-C. Héam, O. Kouchnarenko, and J. Mantovani. *The AVISPA tool for the automated validation of internet security protocols and applications*. in *International conference on computer aided verification*. 2005. Springer.
- [26] Blanchet, B., *A computationally sound mechanized prover for security protocols*. IEEE Transactions on Dependable and Secure Computing, 2008. 5(4): p. 193-207.
- [27] Dolev, D. and A. Yao, *On the security of public key protocols*. IEEE Transactions on information theory, 1983. **29**(2): p. 198-208.
- [28] Wu, F., Xu, L., Kumari, S., & Li, X. (2017). An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. *Multimedia Systems*, 23, 195-205.
- [29] Khan, M. K., & Kumari, S. (2014). An improved user authentication protocol for healthcare services via wireless medical sensor networks. *International Journal of Distributed Sensor Networks*, 10(4), 347169.
- [30] Li, X., Niu, J., Kumari, S., Liao, J., Liang, W., & Khan, M. K. (2016). A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. *Security and Communication Networks*, 9(15), 2643-2655
- [31] He, D., Kumar, N., Chen, J., Lee, C. C., Chilamkurti, N., & Yeo, S. S. (2015). Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. *Multimedia Systems*, 21, 49-60.
- [32] Servati, M. R., Safkhani, M., Ali, S., Malik, M. H., Ahmed, O. H., Hosseinzadeh, M., & Mosavi, A. H. (2022). Cryptanalysis of Two Recent Ultra-Lightweight Authentication Protocols. *Mathematics*, 10(23), 4611.