به نام خدا


**پژوهشکده علوم کامپیوتر**

# پیشنهاد همکاری به عنوان تک پروژه مقیم

**عنوان پروژه:**

# طراحی و تحلیل پروتکل‌های احراز اصالت در محیط‌های با محدودیت منابع

# Design and security analysis of authentication protocols in constraint environments

مجری:

**معصومه صفخانی**

**بهمن ماه ۱۴۰۲**

**عنوان طرح:** طراحی و تحلیل پروتکل‌های احراز اصالت در محیط‌های با محدودیت منابع
**مجری اصلی:** دکتر معصومه صفخانی
**آدرس محل کار:** تهران، لویزان، دانشگاه تربیت دبیر شهید رجایی، دانشکده مهندسی کامپیوتر، گروه نرم افزار

**چکیده:**

با ظهور محیط‌های با محدودیت منبع مانند اینترنت اشـیا و اسـتفاده گسـترده از آن در دنیای امروزی، یکی از چالش‌هایی که با آن روبه‌رو هسـتیم امنیت و حفظ حریم خصـوصـی اسـت. محیط‌های با محدودیت منابع محیط‌هایی هستند که دارای محدودیت (محاسباتی، پردازشی و ذخیره‌سازی) هستند. در این خصوص طرح‌های احرازاصالت بسیاری برای تأمین دسترسی امن پیشنهادشده‌است. این طرح‌های احرازاصالت برای ارائه ویژگی‌های خاصی از قبیل: ناشناس بودن، غیرقابل ردیابی‌بودن، محرمانه بودن، دسترس‌پذیری و یکپارچگی طراحی شده‌اند. از اهداف این طرح‌های امنیتی ارائه یک رویه مبادله‌کلید توافق شـده بین کاربر و سـرور یا یک دروازه اسـت که امنیت را در برابر حملات مختلف فعال و غیر فعال مانند کشـف مقادیر مخفی، رد یابی، جعل هو یت، نقض یکپارچگی، حدس گذرواژه، منع خدمت و غیره را فراهم کند. ما در این پیشـنهاد طرح، تعدادی از طرح‌های امنیتی احرازاصـالت ارائه شـده را مورد ارزیابی قرار داده، و نقاط قوت و ضـعف آنها را از نظر ویژگی‌های امنیتی، حفظ حریم‌خ صو صی و هزینه‌های محا سباتی مورد برر سی قرار خواهیم داد. از طرفی آ سیب‌پذیری 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 بردا شت و پروتکل‌های امنیتی بهبود یافته ارائه خواهند شد و امنیت آنها با ا ستفاده از انواع روش‌های صوری و غیر صوری اثبات خواهد گردید.

**کلید واژه‌ها:** طرح احرازاصالت، محیط با محدودیت منابع، توافق‌کلید، اینترنت‌اشیا، 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 ensure secure access. These authentication schemes are designed to provide special 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 that provides security against various active and passive attacks such as secret disclosure attacks, traceability, impersonation, integrity violations, password guessing, denial of service, etc. In this project proposal, we have evaluated a number of authentication security schemes, and we will examine their strengths and weaknesses in terms of security features, privacy and computing costs. On the other hand, we will identify the vulnerability of the provided protocols against known active and passive attacks and we will take steps to improve security by providing solutions, and improved security protocols will be provided, and their security will be proved using a variety of formal and informal security analysis methods.

**Keywords:** Authentication Scheme, Resources 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[۱]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 یا از ارتباطات بین ماشین لباسشویی و یخچال تا پوشاک وغیره باشد. این شبکه بسیاری از دستگاه‌های اطراف ما را در بر می‌گیرد.


شکل۱: مثالی از شبکه ارتباطی در اینترنت اشیا [۲]

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. همان‌طورکه ارتباط بین یک تلفن همراه/کارت هوشمند در یک شبکه عمومی اتفاق می‌افتد، می‌توان نتیجه گرفت که کل سامانه، آسیب‌پذیر در مقابل تهدیدات امنیتی است که مربوط به شبکه عمومی می باشد. حفظ حریم خصوصی و به ویژه ناشناس بودن از مهم ترین ویژگی هایی است که باید در پیاده‌سازی یک سامانه الکترونیکی در سطح جهانی که در [۲] به آن اشاره شده است، در نظر گرفته شود.

## ۲-پیشینه تحقیق:

پروتکل‌های احرازاصالت و توافق‌کلید بسیاری نظیر[ ۱-۳۲] تاکنون برای محیط‌های با محدودیت منابع ارائه‌شده‌است. در واقع یک پروتکل احرازاصالت راه تعامل و ارتباطی بین کاربر و سرور است که خود شامل مراحل مختلفی است. یک پروتکل احرازاصالت 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

## ۲-۱پروتکل وینود و همکاران[1]

رایانش ابری خودرویی یا (VCC[2]) که یک زمینه تحقیقاتی نوظهور محسوب‌می‌شود 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 احرازاصالت شامل سه مرحله می‌باشد. مرحله ۱) ثبت‌نام، مرحله ۲) ورود و احراز اصالت و مرحله ۳) تغییر رمز عبور. در این طرح احرازاصالت از نمادها و علائمی استفاده می‌شود که در جدول ۱ نشان داده‌شده‌است.

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

| Symbol | Description | Symbol | Description |
|---|---|---|---|
| $T_i$ | $i$th RFID tag | $pw_T$ | 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 | $\Delta T$ | Maximum time delay in comunication |
| $l$ | 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 | $\|$ | Concatenation operation |
| $SK_{ij}(.)$ | 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 |
| $i \cdots \Rightarrow j : \{M\}$ | $i$ sends message $M$ to $j$ via secure channel | $i \cdots \rightarrow j : \{M\}$ | $i$ sends message $M$ to $j$ via public channel |
| RP | Registration phase | LAP | Login and authentication phase |

### مرحله ثبت‌نام در پروتکل وینود و همکاران

دراین مرحله، برچسب مقادیری مانند شناسه و رمزعبور 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 $R_T$ و $T_{R1}$ به ترتیب نشان دهنده عدد تصادفی تولید شده توسط برچسب و زمان جاری[3]است.

$$PWT = h(ID_T \parallel PW_T \parallel R_T)$$
$$M_{R1} = \{PWT, ID_T, T_{R1}\}$$

به محض دریافت پیام فوق، سرور زمان دریافت شده را با زمان فعلی خود مقایسه می‌کند، یعنی $T_{R2} - T_{R1} \leq \triangle T$. اگر این مقدار بررسی شده صحیح باشد، روند ثبت نام ادامه پیدا می‌کند در غیر این‌صورت روند ثبت‌نام متوقف می‌شود. سپس سرور یک مقدار تصادفی به نام $sn_i$ را تولید می‌کند و درنهایت 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 $M_{R2} = \{B_T, A_T, sn_i, g, xsg, G, h(.)\}$ به برچسب ارسال می‌شود.

[1]-Vinod et al.
[2]-Vehicular cloud computing (VCC)
[3]-Timestamp

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

| Tag $T_i$ | Cloud database server $S$ |
|---|---|
| Inputs $ID_T$ and $pw_T$ | |
| Generates $R_T \in Z_q^\star$ | |
| Computes $PWT = h(ID_T \| pw_T \| R_T)$ | |
| Sends $M_{R1} = \{PWT, ID_T, T_{R1}\}$ | |
| ·····⇒ | Verifies $T_{R2} - T_{R1} \leq \Delta T$ |
| | Generates $sn_i \in Z_q^\star$ |
| | $sn_i$ 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 $M_{R2} = \{B_T, A_T, sn_i, g, x_S g, G, h(.)\}$ |
| | ⇐····· |
| Store $\{B_T, A_T, R_T, sn_i, g, x_S g, G, h(.)\}$ in database | |

شکل ۲: مرحله ثبت‌نام در پروتکل وینود 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:

$$PWT^/ = h\left(ID_T^/ \| PW_T^/ \| R_T^/\right)$$
$$X_T^* = B_T \oplus PWT^/$$
$$A_T^* = h(PWT^/ \| X_T^* \| ID_T)$$

سپس مقادیر $A_T^* = A_T$ مقایسه می‌شود. در صورت صحت این رابطه روند پروتکل ادامه می‌یابد. در غیر این‌صورت رویه متوقف می‌شود. بدین صورت، در صورت تساوی ذکر شده یک عدد تصادفی به نام $ag \in z_q^*$ تولید شده و مقدار $W_1 = h(X_T^* \| ag \| ID_T)$ محاسبه می‌شود 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 تاخیرزمانی را بررسی می‌کند $T_{LA2} - T_{LA1} \leq \triangle T$ 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 $T_{LA4} - T_{LA3} \leq \triangle T$ 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.

$$SK_{ST} = h(ID_T^* \| X_T \| bag \| xsag \| sn_i \| T_{LA5})$$
$$W_2 = h(ID_T^* \| SK_{ST} \| bg \| T_{LA5})$$

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

گام پنج) مقدار تاخیر زمانی $T_{LA8} - T_{LA7} \leq \triangle T$ توسط برچسب بررسی می‌شود. سپس کلید نشست $SK_{TS}$ توسط برچسب محاسبه می‌گردد و مقدار $W_2^*$ نیز مورد راستی‌آزمایی قرار می‌گیرد که در صورت صحت این مقدار روند ورود و احراز اصالت با موفقیت به پایان می‌رسد.

$$SK_{TS} = h(ID_T \parallel X_T^* \parallel abg \parallel axsg \parallel sn_i \parallel T_{LA7})$$
$$W_2^* = h(ID_T \parallel SK_{ST} \parallel bg \parallel T_{LA7})$$

**مرحله تغییر رمزعبور**

گام یک) برچسب مقادیر $pw_T^/$ ، $ID_T^/$ و $R_T^/$ را وارد می‌کند و سپس مقادیر زیر توسط برچسب محاسبه می‌شود:

$$PWT^/ = h\left(ID_T^/ \parallel PW_T^/ \parallel R_T^/\right)$$
$$X_T^* = B_T \oplus PWT^/$$
$$A_T^* = h(PWT \parallel X_T^/ \parallel ID_T^/)$$

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

گام دو) در این مرحله، مقدار رمزعبور همراه با یک عدد تصادفی جدید وارد می‌شود و سپس مقادیر زیر محاسبه می‌شود.

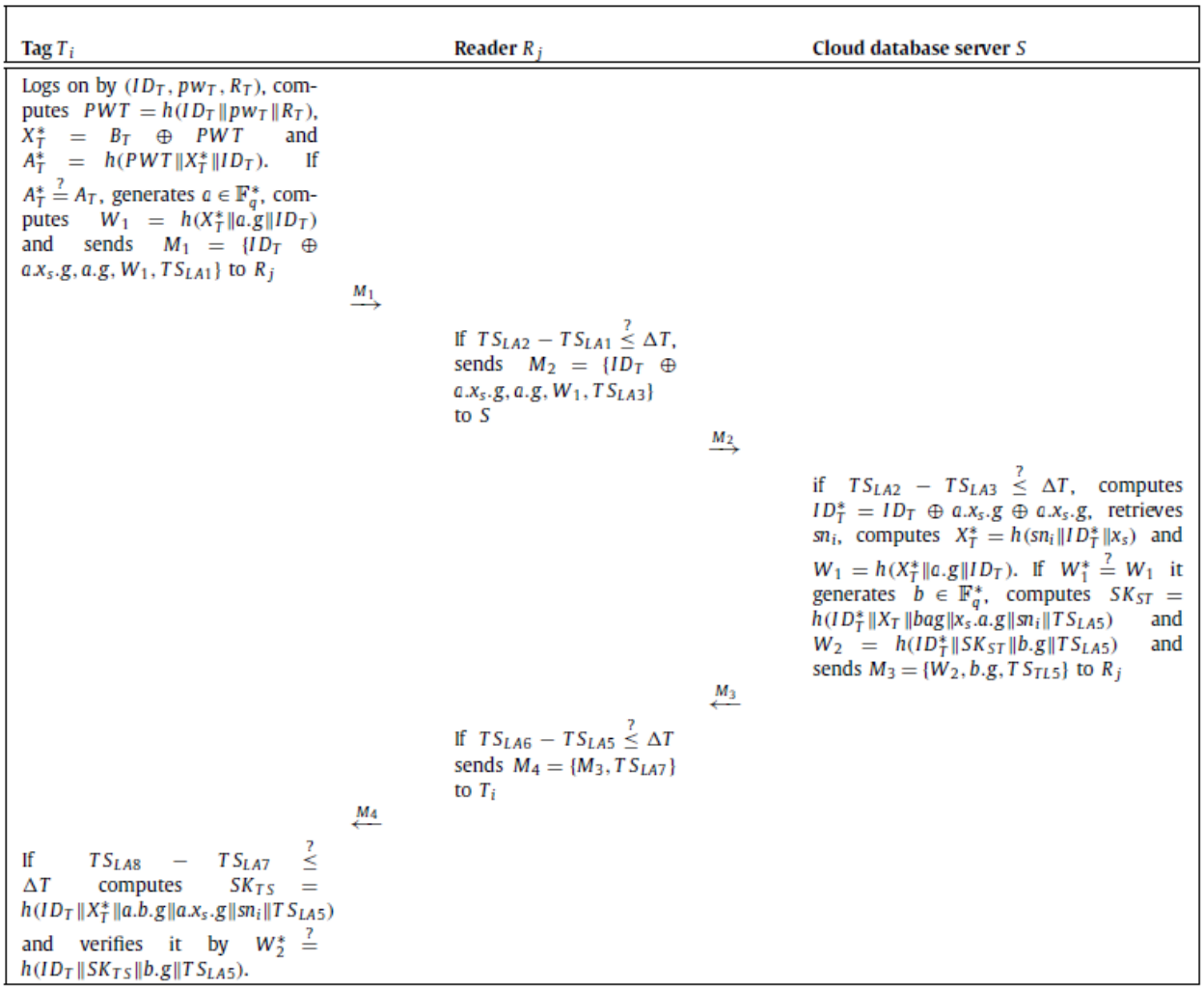
$$PWT^{NEW} = h(ID_T \parallel PW_T^{NEW} \parallel R_{NEW})$$
$$X_T^{NEW} = B_T \oplus PWT^{NEW}$$

گام سه) برچسب مقدار $PW_T$ را با $PW_T^{NEW}$ و $PWT^{NEW}$ را با $PWT$ و $X_T^{NEW}$ را با $X_T$ به ترتیب عوض می‌کند.

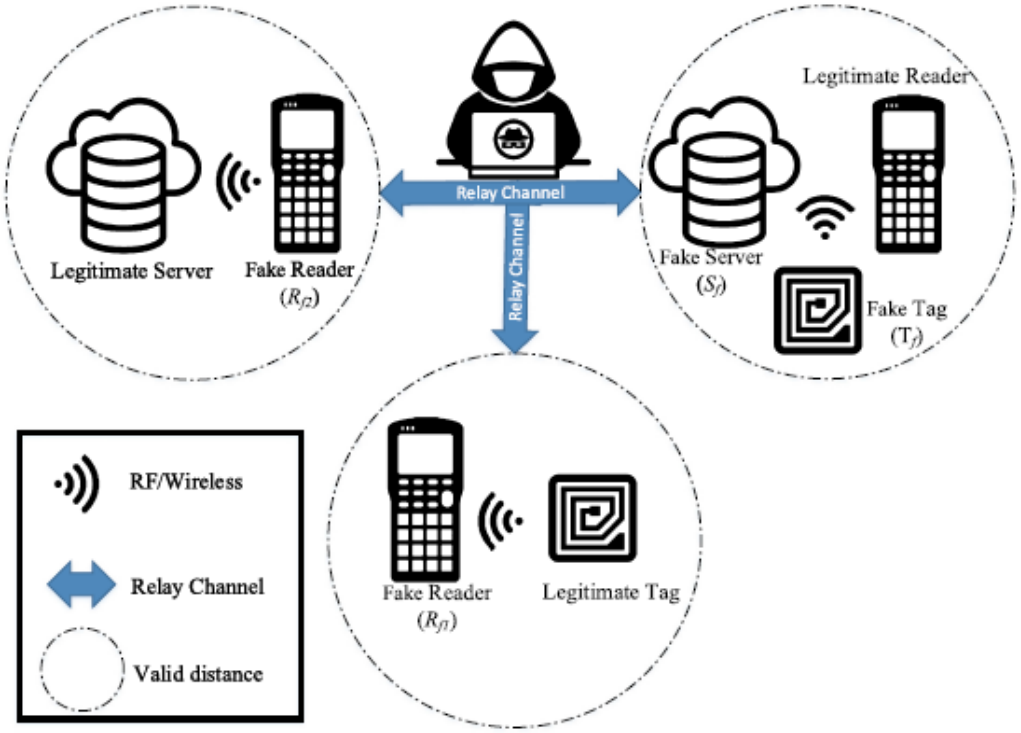
**پروتکل بهبودیافته وینود و همکاران**

در بررسی‌های انجام شده پروتکل شرح داده شده دارای احراز اصالت دو طرفه و در برابر حملات شناخته شده‌ای 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 پروتکل [۱۵] در برابر حمله رله[1] حمله جعل برچسب مقاوم نیست و در شکل ۳ طرح بهبود یافته مرحله ورود و احراز اصالت آن را مشاهده می‌کنیم که توسط صفخانی و همکاران [۱۶] ارائه شده است. نکته مهم در حمله رله پیشنهادی علیه وینود و همکاران، حملات جعل هویت موفق و همچنین نقص در یکپارچگی مهر زمانی مورد استفاده در پروتکل است. تحلیل امنیتی صوری پروتکل بهبود یافته با استفاده از ابزار AVISPA و نیز منطق BAN انجام شده‌است. در ادامه قصد داریم حمله رله و جعل برچسب ارائه شده بر علیه پروتکل وینود و همکاران را شرح دهیم.

[1]-Relay attack




شکل ۳: مرحله ورود و احرازاصالت پروتکل بهبود یافته صفخانی و همکاران [۱۶]




شکل ۴: حمله رله بین برچسب و قرائت‌گر[۱۶]

**حمله رله بر علیه پروتکل وینود و همکاران**

همان طور که در شکل۴ 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 قرائت گر 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 و $W_2$ 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 درصورت 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 $T_i$ و 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. از این رو، دشمن با موفقیت وکارآمدی یک حمله رله را بر علیه پروتکل وینود و همکاران انجام داده است. بنابراین، پس از این حمله، دشمن همچنین می‌تواند پیام‌های 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 قرائت‌گرتقلبی 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 به‌جای $T_{LA1}$ یک مقدار دیگر مانند $T'_{LA1}$ را استفاده کند، از آنجایی که نه تنها قرائت‌گر بلکه سرور نیز یکپارچگی این مقدار را تشخیص نمی‌دهند، بنابراین مقدار زمانی مهاجم را یک مقدار قابل اعتماد یا معتبر می‌پندارند، 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[1]**

در [۱۷] یک طرح آدرس‌دهی و احراز اصالت امن (SCSAA[2]) مبتنی بر کارت هوشمند با اصلاح پروتکل IPV6 استاندارد برای کاهش تهدیدات امنیتی در اینترنت اشیا پیشنهادشده‌است. طرح پیشنهادی دارای دو قسمت است. در مرحله اول، این طرح با اختصاص شناسه رابط ۶۴ بیتی منحصر به فرد ID 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 انجام‌شده‌است. 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 داده‌شده‌است. پروتکل چوهان وکومار دارای ۱- مرحله ثبت‌نام، ۲- مرحله ورود، احرازاصالت و توافق کلید و ۳-مرحله به هنگام‌رسانی رمز عبوراست.

**مرحله ثبت‌نام**

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

[1]-Pankaj Kumar, Lokesh Chouhan
[2]-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 |
| $PWi$ | Password identity of the user |
| \|\| | Concatenation operation |
| h() | Hash function |

| User (U) | Edge server (ENS) |
|---|---|
| STEP 1: Chosen an identity $(IID_u \| IID_{ens} \| IID_{ug} \| T_{id})$ | |
| | 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 $P_{IID}$ Computes $B = h(IID_u \| N \| T_{id})$ and store $(IID_u, T_{id})$ in key table Assign the unique identities using *smart card* SC $= h(IID_u \| IID_d)$ and send to the user |
| STEP 3: Compute C $= h(Bi \| PW_i)$ then computes $SC = h(IID_u \| IID_d \| C)$, Compute A $= B \oplus h(PW_i \| IID_u \| T_{id})$ Compute R $= h(A \| IID_u \| T_{id} \| SC)$ 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 $(PW_i \| IID_{u \| Bio_i})$ 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 $B_1 = h(IID_u \| N \| T_{id}, Token_{id}, SK_{SHS})$ and send using secret key to user end to the user. |

شکل ۵: مرحله شروع و ثبت‌نام 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 می‌دهد.

| User (U) | Smart home server (SHS) |
|---|---|
| STEP 1: Insert the smart card<br>Enter $ID_u$, $PW_i$, $Bio_i$<br>Verify if A′ = $A$<br>else verify R′ = $R$<br>Compute $IID = h(IID_u \| IID_d)$<br>F= $h(IID \| PW_i, B_i)$<br>M= $N_1 \oplus h(F \| IID)$<br>Compute $A_1 = B \oplus h(M \| PW_i \| IID \| T_{id} \| SK_{SHS} \| Token_{id})$<br>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.<br>Generates random number N<br>chose pseudo identity $P_{ID}$<br>Computes $B = h(ID_u \| N \| T_{id} \| IID_u \| IID_d)$ and store $(ID_u, T_i)$ in key table<br>Granted the $Token_{id}$ and $SK$.<br>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 $h(IID_u \| IID_d$<br>Compute K = $h(U_{sid} \| PW_i \| SHS_{sid})$<br>Compute S = $h(IID \| PW_i \| SK \| N_2)$<br>Compute V = $S \oplus h(IID \| T_{id} \| SK \| N2)$<br>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.<br>Compute $(U_{sid} \| SHS_{sid})$<br>Compute $U_{sid} = (V \oplus h(IID \| SK \| N_2))$<br>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 رمزعبور

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 خود کرده و با وارد کردن اطلاعات منحصر به فرد خود، وارد سامانه می‌شود. کارت هوشمند، مقدار $h(IID_u \parallel IID_d)$ را محاسبه می‌کند و از سرورگره خانه می‌خواهد تا رمز عبور خود را با کمک $PC = h(PW_i \parallel IID_u \parallel IID_d \parallel Bio_i)$ 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 گذرواژه برون‌خط، حمله نقض امنیت پیشرو، حمله مردمیانی، حمله تغییر رمزعبور، حمله ردیابی، حمله جعل‌پیام،

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.

### ۲-۳ پروتکل پیشنهادی کومارپاندا و چپتاپدهی[1]

در [۱۸] یک پروتکل احرازاصالت امن برای محیط اینترنت اشیاء و سرورهای ابری بر اساس رمزنگاری منحنی بیضوی پیشنهادشده‌است. 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 حدس‌زدن رمزعبور، برآورده نمودن احراز اصالت متقابل و غیره مقایسه‌شده‌است. علاوه بر این، عملکرد پروتکل پیشنهادی از نظر هزینه های محاسباتی، ارتباطاتی، سربار ذخیره‌سازی و کل زمان اجرا نیز ارزیابی‌شده‌است. تجزیه و تحلیل امنیتی و عملکردی انجام شده در [۱۸] برتری پروتکل کومارپاندا و چپتاپدهی 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.

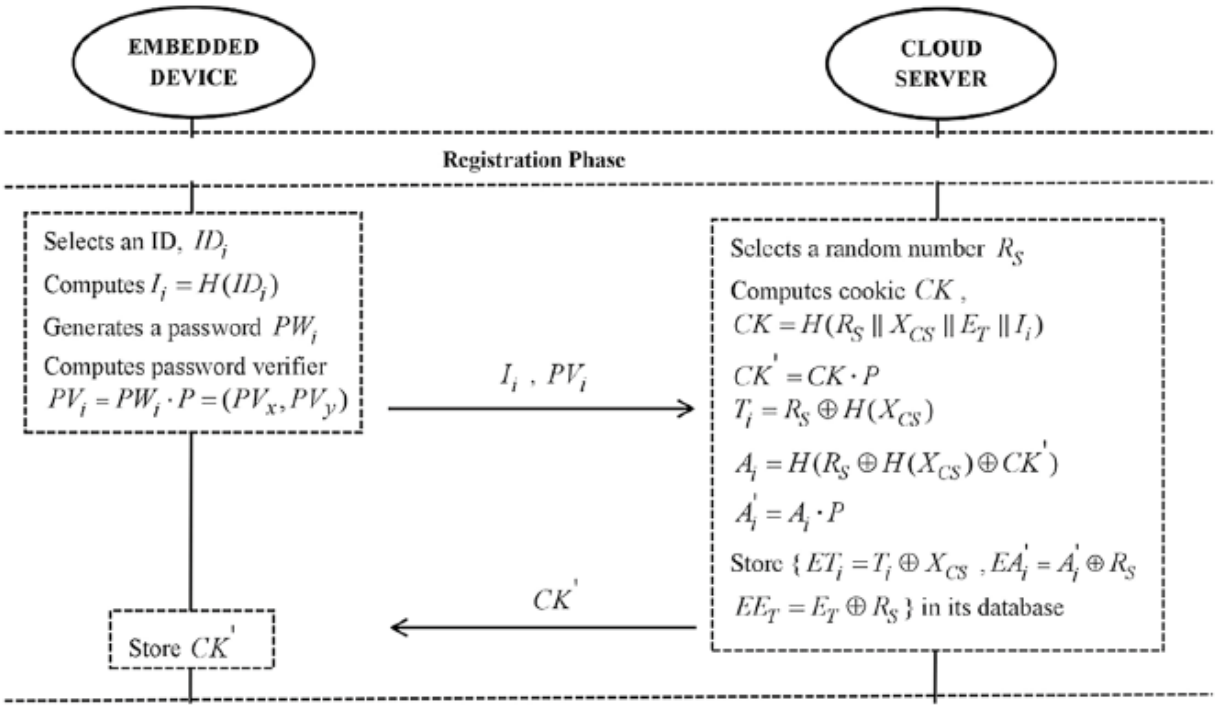
جدول ۳: علائم و نشانه‌های استفاده شده در پروتکل کومارپاندا و چپتاپدهی[۱۸]

| 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 چپتاپدهی

شکل ۸ مرحله ثبت‌نام در پروتکل کومارپاندا و چپتاپدهی را نشان‌می‌دهد.

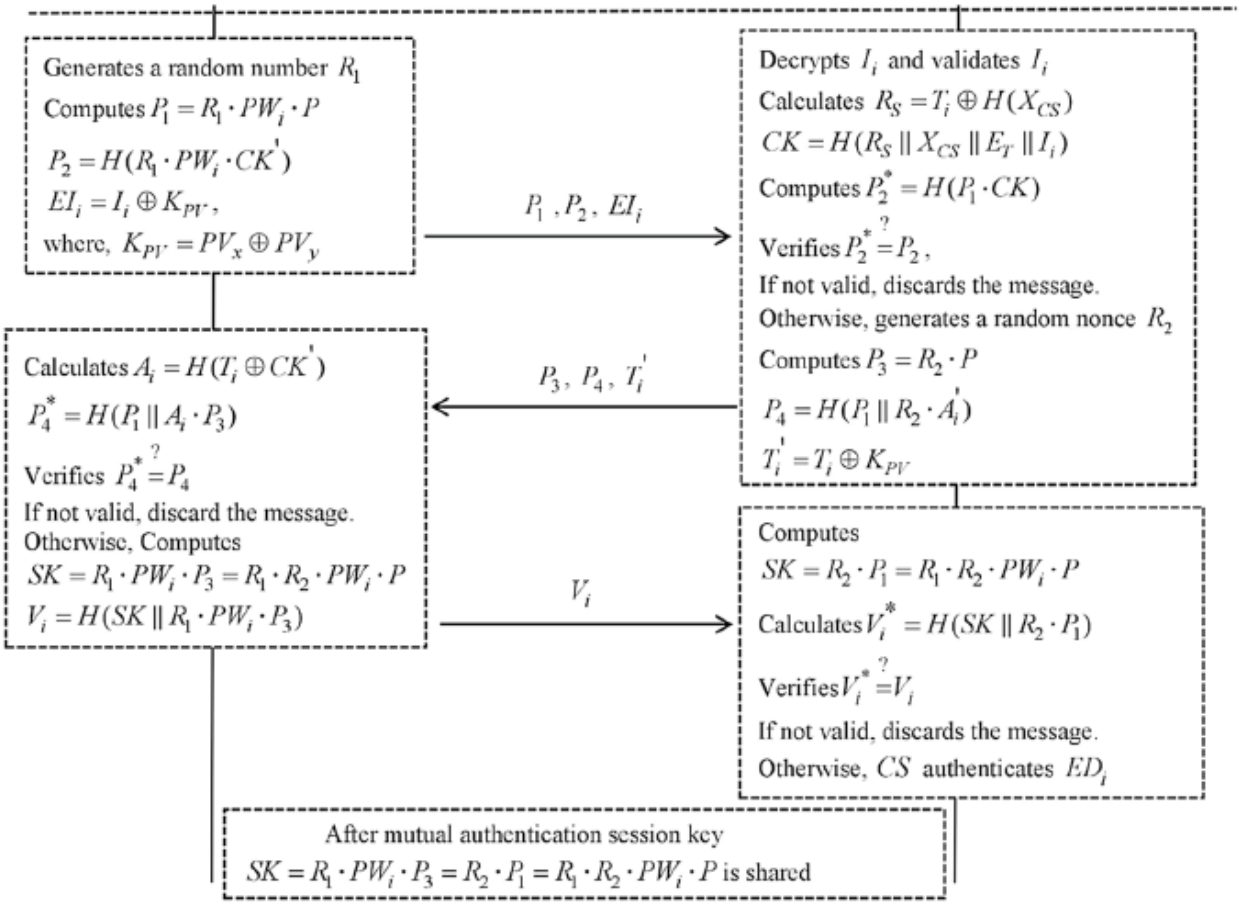
[1]- Prabhat Kumar Panda, Sudipta Chattopadhyay




شکل ۸: مرحله ثبت‌نام در پروتکل کومارپاندا و چپتاپدهی[۱۸]

**مرحله ورود و احراز اصالت در پروتکل کومارپاندا و چپتاپدهی**

شکل ۹ مرحله ورود و احرازاصالت در پروتکل کومارپاندا و چپتاپدهی را نشان‌می‌دهد.




شکل ۹: مرحله ورود و احرازاصالت در پروتکل کومار پاندا و چپتاپدهی [۱۸]

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

### ۲-۴ طرح احرازاصالت سونگاتی و همکاران

علائم حیاتی و پارامترهای فیزیولوژیکی بیمار را می‌توان با گره‌های حسگر متصل به شبکه حسگر بدن بیمار کنترل کرد و سپس از طریق رسانه‌های ارتباط بی‌سیم مانند بلوتوث، WiFi، 3G/4G به پزشک متخصص مربوطه منتقل کرد. در عین حال، امنیت و حریم خصوصی داده‌های 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 می‌کند که امکان نظارت مستمر بر بیمار را حتی در یک محیط غیربالینی فراهم می‌کند. علاوه بر این، این طرح شامل یک مرحله برای سناریوی اضطراری است که به موجب آن کیفیت مراقبت از بیمار در شرایط بحرانی حفظ می‌شود. تحلیل امنیتی انجام شده در[۱۹] نشان می‌دهد که طرح پیشنهادی در مقایسه با سایر طرح‌های مرتبط اخیر کارآمدتر است. پروتکل پیشنهادی سونگاتی و همکاران شامل مراحل زیر است: ۱) ثبت‌نام، ۲) ورود به سامانه و احراز اصالت، ۳) تغییر رمزعبور و ۴) سناریوی اضطراری . جدول ۴ نمادهای به کار برده شده را در پروتکل سونگاتی و همکاران[۱۹] را نشان می‌دهد.

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

| Notation | Description |
|---|---|
| $SN_k$ | Sensor node $k, k = 1, 2, 3 \ldots, n$ |
| $ID_{SN_k}$ | Identity of sensor node $k$ , $k = 1, 2, 3 \ldots, n$ |
| $ID_U$ | 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 ثبت‌نام کاربر در پروتکل سونگاتی و همکاران

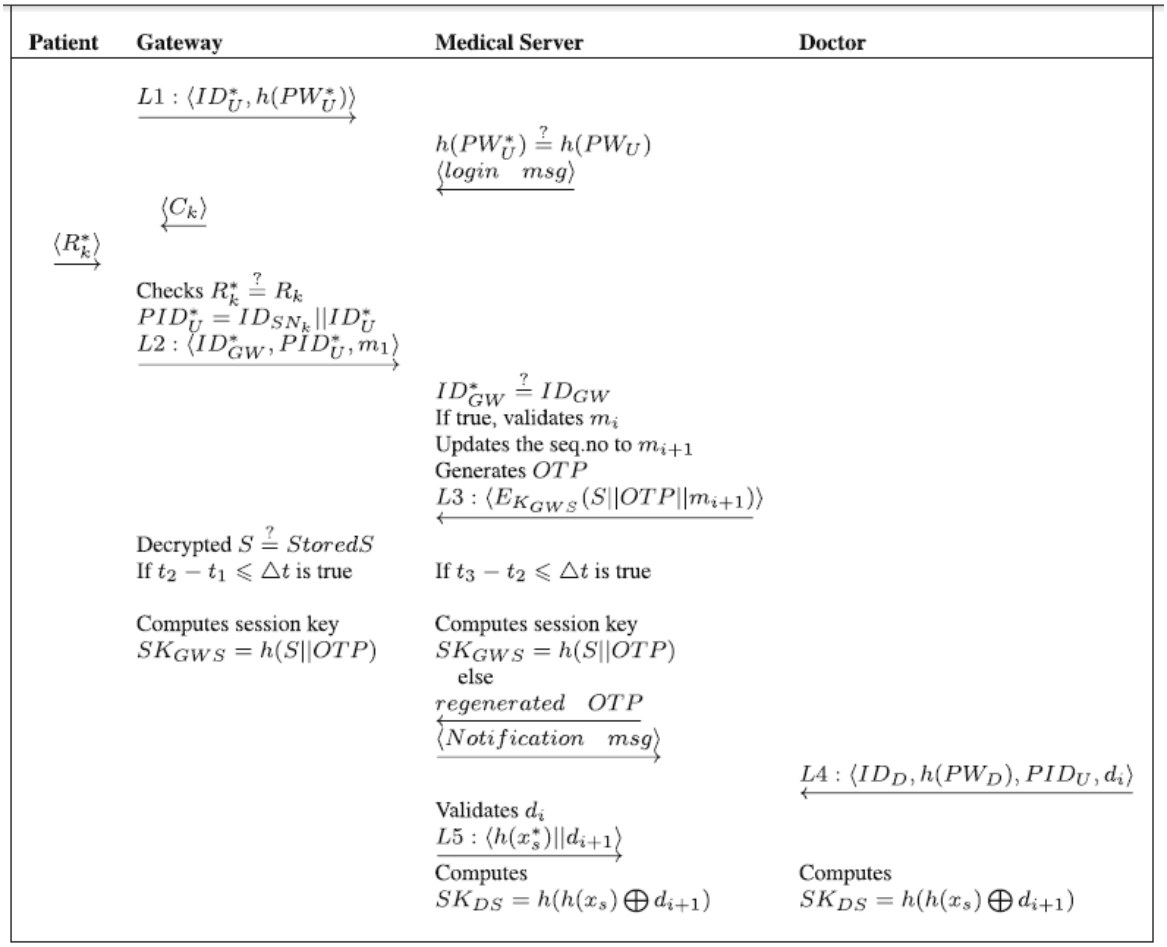
شکل ۱۰ مرحله ثبت‌نام کاربر را در پروتکل سونگاتی و همکاران را نشان‌می‌دهد.

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

شکل ۱۰: مرحله ثبت‌نام 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 ۱۱نشان داده‌شده‌است.




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

**مرحله تغییر رمزعبور در پروتکل سونگاتی و همکاران**

در این طرح هر زمان که بیمار بخواهد رمز عبور $PW_U$ را با رمز ورود $(pw_U)_{NEW}$ جدید 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 تأییدکند. 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 ثبت‌نام، لیست پزشکان، خدمات آمبولانس و شماره تماس آن‌ها را به بیمار ارائه‌می‌دهد. علاوه بر این، دروازه دامنه معتبری از داده‌ها را برای هر یک از حسگرهایBSN ذخیره می‌کند. هنگامی‌که بیمار در گره دروازه ثبت‌نام 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 در شبکه حسگر بدن بیمار (BSN)

[1]-Body Sensor Network

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، تنگی‌نفس، کمردرد، بی‌حسی/ ضعف، تغییردر بینایی، دشواری درگفتار باشد 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 |
| Above180 | 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 دربرابر حملاتی مانند افشای کلید نشست، حمله تکرار، حمله حدس برون/درون خط رمزعبور، جعل هویت‌کاربر، 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[1]

پروتکل CoAP[2]، 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[3] مرتبط است و بر اساس معماری انتقال حالت کار می‌کند. CoAP با پروتکل DTLS[4] 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 درلایه DTLS در CoAP وجود دارد. برای غلبه بر محدودیت‌های موجود مربوط به مدیریت کلید و امنیت چندرسانه ای 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. CoAP پیشنهادی مبتنی بر ECC به عنوان ECC-CoAP[5] نامیده می‌شود که پیاده سازی CoAP را برای احراز اصالت در شبکه اینترنت اشیا ارائه 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، مرحله چالش احراز

[1]-Majumder et al.
[2]-Constraint Application Protocol
[3]-User datagram protocol
[4]-Datagram transport layer security
[5]-Elliptic Curve Cryptography Based Constraint Application Protocol

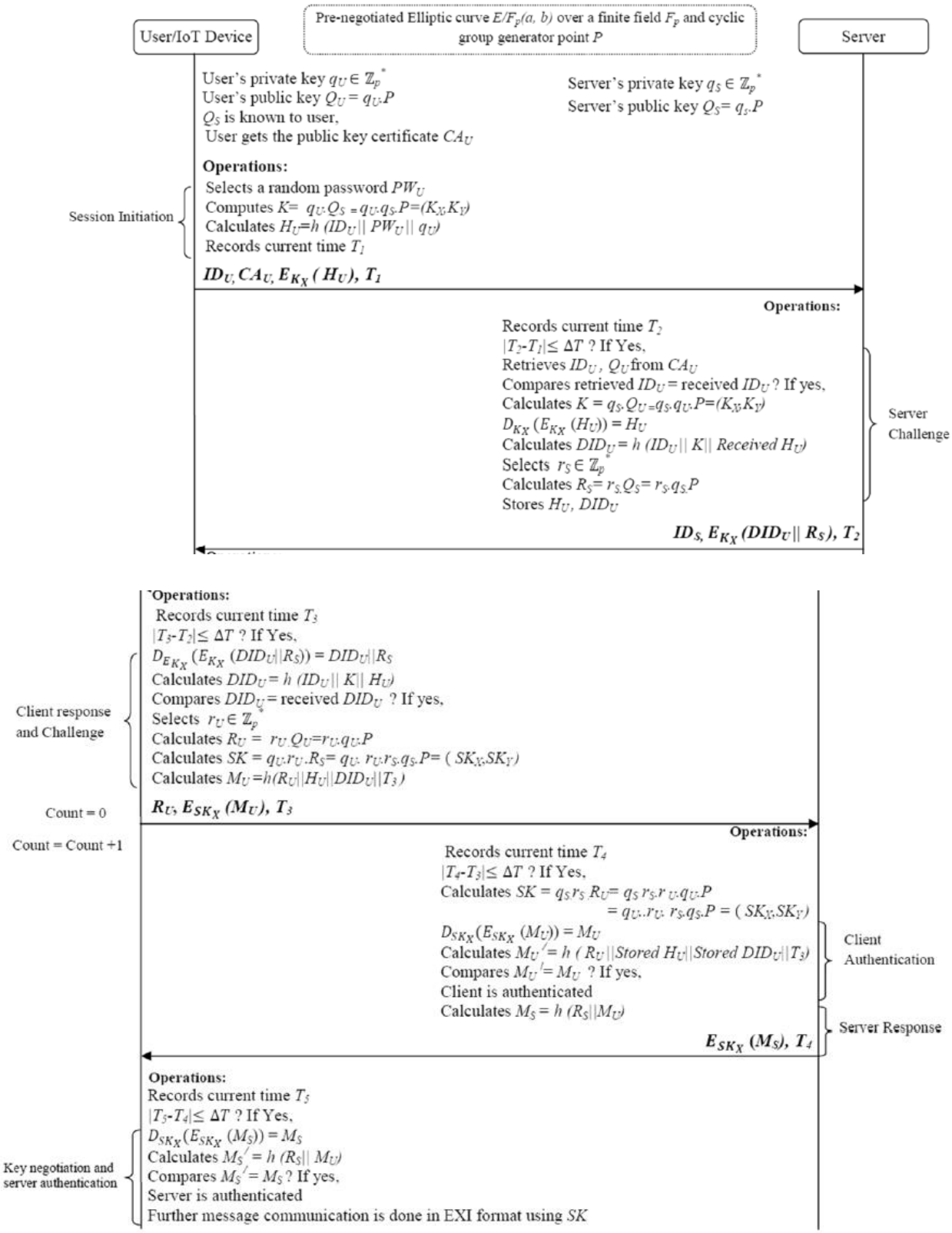
اصالت‌کاربر، مرحله پاسخ سرور و مرحله مذاکره کلید و احراز اصالت سرور است. جدول ۶ نمادهای به کار برده شده در پروتکل مجمودار و همکاران را نشان می‌دهد.

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 $R_U=r_U.Q_U$ |
| $R_S$ | Random value produced by the server where $R_S=r_S.Q_S$ |
| $h(.)$ | One way secure hash function such as *SHA1* |
| $E/D$ | Symmetric encryption/decryption algorithm |
| $(q_S, Q_S)$ | Private–public key pair of server where $Q_S=q_S.P$ |
| $(q_U, Q_U)$ | Private–public key pair of user/IoT device where $Q_U=q_U.P$ |
| $\|$ | Concatenation |

مراحل مختلف پروتکل مجمودار و همکاران [۲۰] در شکل ۱۲ نشان داده شده است. مراحل انجام 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 احرازاصالت رخ می‌دهد و درنهایت یک توافق کلید و احرازاصالت بین فرستنده و گیرنده رخ می‌دهد.

در [۲۰] بیان شده‌است که پروتکل مجمودار و همکاران دارای خاصیت احراز اصالت متقابل است و در برابر حملاتی مانند حمله مردمیانی، حمله منع‌خدمت، حمله تکرار، حمله داخلی، حمله جعل هویت‌کاربر، حمله جعل هویت سرور، حمله حدس رمز عبور برون‌خط، حمله محاسبه کلید نشست و حمله نقض امنیت پیشرو مقاوم است.




شکل ۱۲: مرحله ثبت‌نام و احرازاصالت در پروتکل مجمودار و همکاران[۲۰]

### ۲-۶ طرح احرازاصالت کال و آوستی

کال و آوستی یک پروتکل احراز اصالت را در [۲۱] مناسب محیط‌های دارای محدودیت منابع ارائه کرده‌اند. آنها ادعا کردند که پروتکل معرفی شده آنها برای کاربردهایی در دنیای واقعی کارآمد و ایمن است. بعد از آن رانا و همکاران در [۲۲] نشان داد 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 معرفی‌کند و از خدمات ارائه شده توسط سرور بهره ببرد. بنابراین، پروتکل کال و آوستی مستعد حملات جعل هویت‌کاربر 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 هویت‌کاربر 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 رمزعبور 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 |
| $\delta T$ | Expected time interval for a transmission delay |
| $h(.)$ | Secure one way hash function $h(.) : \{0,1\}^* \rightarrow \{0,1\}^{128}$ |
| $\oplus$ | Bitwise XOR operation |
| $\|$ | Concatenation operation |

#### مرحله ثبت‌نام، ورود و احرازاصالت در پروتکل کال و آوستی

مراحل ثبت‌نام، ورود و احراز اصالت و تغییر رمزعبور 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 $RPW_i = h(b\|\|PW_i)$ | |
| $\xrightarrow[ID_i, RPW_i]{}$ | |
| | 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 $\{\beta_i, \gamma_i, \chi_i, h(.)\}$ on smart card |
| | $\xleftarrow{SmartCard}$ |
| Compute $\eta_i = b \oplus h(ID_i \oplus PW_i)$ | |
| Store $\{\eta_i\}$ on smart card | |

شکل ۱۳: مرحله ثبت‌نام 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 $\omega_i = y_i \oplus h(ID_i \oplus \alpha_i) \oplus h(ID_i \oplus \alpha_i \oplus T)$ | |
| | $\vartheta_i = h(ID_i\|\|\alpha_i\|\|y_i\|\|(\alpha_i \oplus y_i)\|\|T)$ | |
| | $\xrightarrow[ID, \omega_i, \vartheta_i, T]{}$ | |

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 رمزعبور در پروتکل کال و آوستی [۲۱]

همانطور که اشاره شد، پروتکل کال و آوستی دربرابر حمله جعل مقاوم نیست، از این‌رو رانا و همکاران در [۲۲] پروتکلی را بهبود طرح آنها ارائه‌دادند. در پروتکل رانا و همکاران ادعا شده‌است که دربرابر طیف وسیعی از حملات مقاوم است.

**حمله جعل بر علیه پروتکل کال و آوستی**

مهاجم درخواست احرازاصالت یک کاربر را شنود می‌کند $\{ID_c, W_c, V_c, T_1\}$ تا اطلاعات آن نظیر $\{ID_c, U_c\}$ را به‌دست آورد. سپس با انتخاب یک رمزعبور $PW_a$ و یک مقدار دلخواه مثل $m_a$ مقدار $RPW_a$ را به صورت $RPW_a = h(m_a \| PW_a)$ محاسبه می‌کند و سپس درخواست ثبت‌نام $\{RPW_a, ID_c\}$ را برای سرور ارسال می‌کند.

سرور با دریافت اطلاعات فوق، مقادیر زیر را محاسبه می‌کند:

$a_c = h((ID_c \oplus a)|b)$
$B_a = a_c \oplus h(ID_c \oplus RPW_a)$
$Y_a = y_a \oplus h(a_c \oplus RPW_a)$
$X_a = h(ID_c|RPW_a|y_a|a_c)$

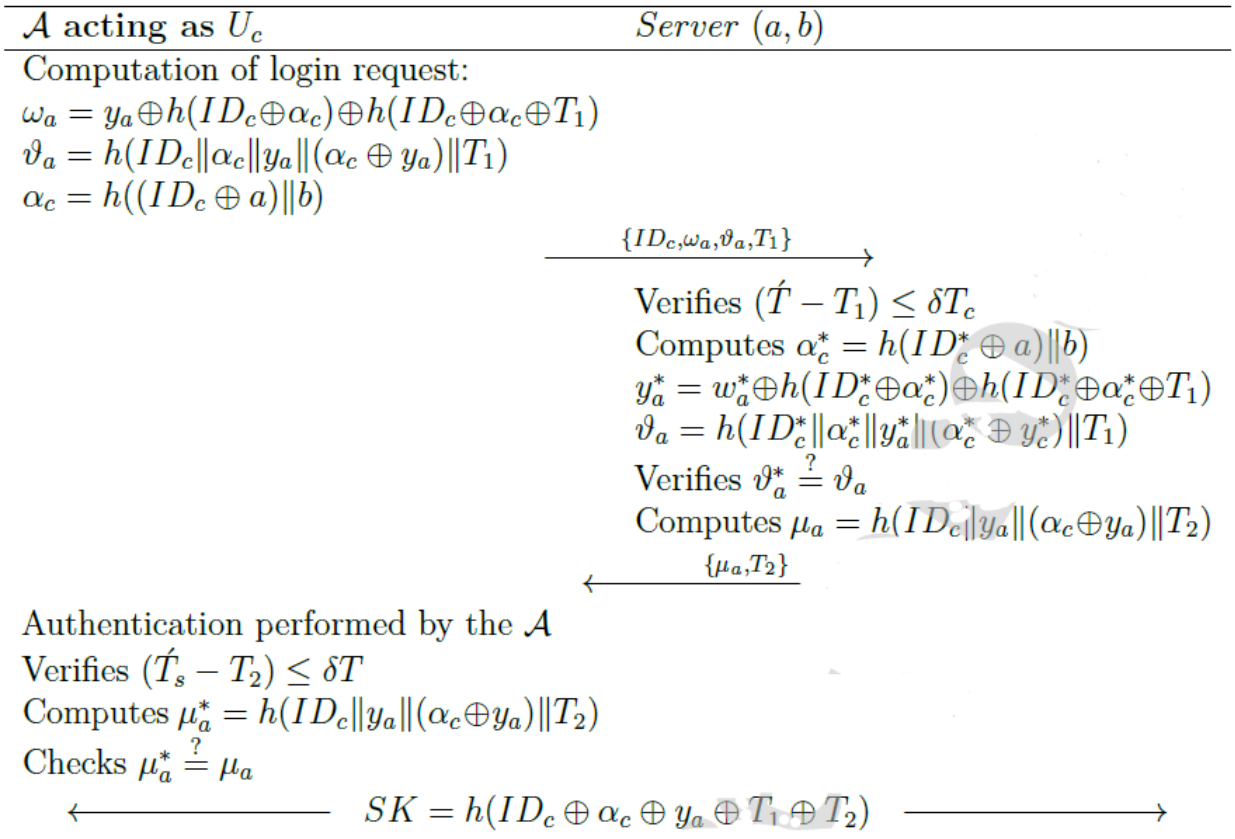
سپس سرور اطلاعات $\{X_a, B_a, Y_a, h(.)\}$ را در کارت هوشمند ذخیره می‌کند و برای مهاجم ارسال می‌کند.

مهاجم بعد از دریافت اطلاعات فوق، مقادیر $\{X_a, B_a, Y_a, h(.)\}$ را استخراج می‌کند و سپس مقادیر $a_c, y_a$ را به صورت زیر بازیابی می‌کند.

$a_c = B_a \oplus h(ID_c \oplus RPW_a)$
$y_a = Y_a \oplus h(a_c \oplus RPW_a)$

که در آن $RPW_a = h(m_a \| PW_a)$ است. بدین صورت با داشتن $y_a$ و $a_c$ یک مهاجم می‌تواند یک کاربر را جعل کند.

لازم به ذکراست که شکل ۱۷ نمایی از حمله جعل وارده بر پروتکل کال و آوستی را نشان‌می‌دهد.




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

### ۲-۷ طرح احرازاصالت 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 وهمکاران شامل چهار مرحله است: مرحله ثبت‌نام، مرحله ورود به سامانه، مرحله احرازاصالت و مرحله تغییر رمز عبور.

**مرحله ثبت نام در طرح احرازاصالت رانا و همکاران**

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

| $User\ \mathcal{U}_c$ | $Server\ \mathcal{S}$ |
|---|---|
| Choose $ID_c$ and $PW_c$ | |
| Choose an arbitrary number m | |
| Compute $RPW_c = h(m\|PW_c)$ | |
| | $\xrightarrow{\{ID_c, RPW_c\}}$ |
| | Selects an arbitrary number $y_c$ |
| | $\boxed{\overline{DID_c} = Enc_{ds}(ID_c\|y_c)}$ |
| | Compute $\alpha_c = h((ID_c \oplus a)\|b)$ |
| | $\beta_c = \alpha_c \oplus h(ID_c \oplus RPW_c)$ |
| | $\gamma_c = y_c \oplus h(\alpha_c \oplus RPW_c)$ |
| | $\chi_c = h(ID_c\|RPW_c\|y_c\|\alpha_c)$ |
| | Stores$\{\ \beta_c, \gamma_c, \overline{DID_c}, \chi_c, h(.)\}$ on $SC_c$ |
| | $\xleftarrow{\{SC_c\}}$ |
| Compute $\eta_c = m \oplus h(ID_c \oplus PW_c)$ | |
| Store $\{\eta_c\}$on $SC_c$ | |

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

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

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

**مرحله تغییر رمزعبور در طرح احراز اصالت رانا و همکاران**

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

کارت‌خوان 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، کارت‌خوان هوشمند مقادیر زیر را استخراج می‌کند.

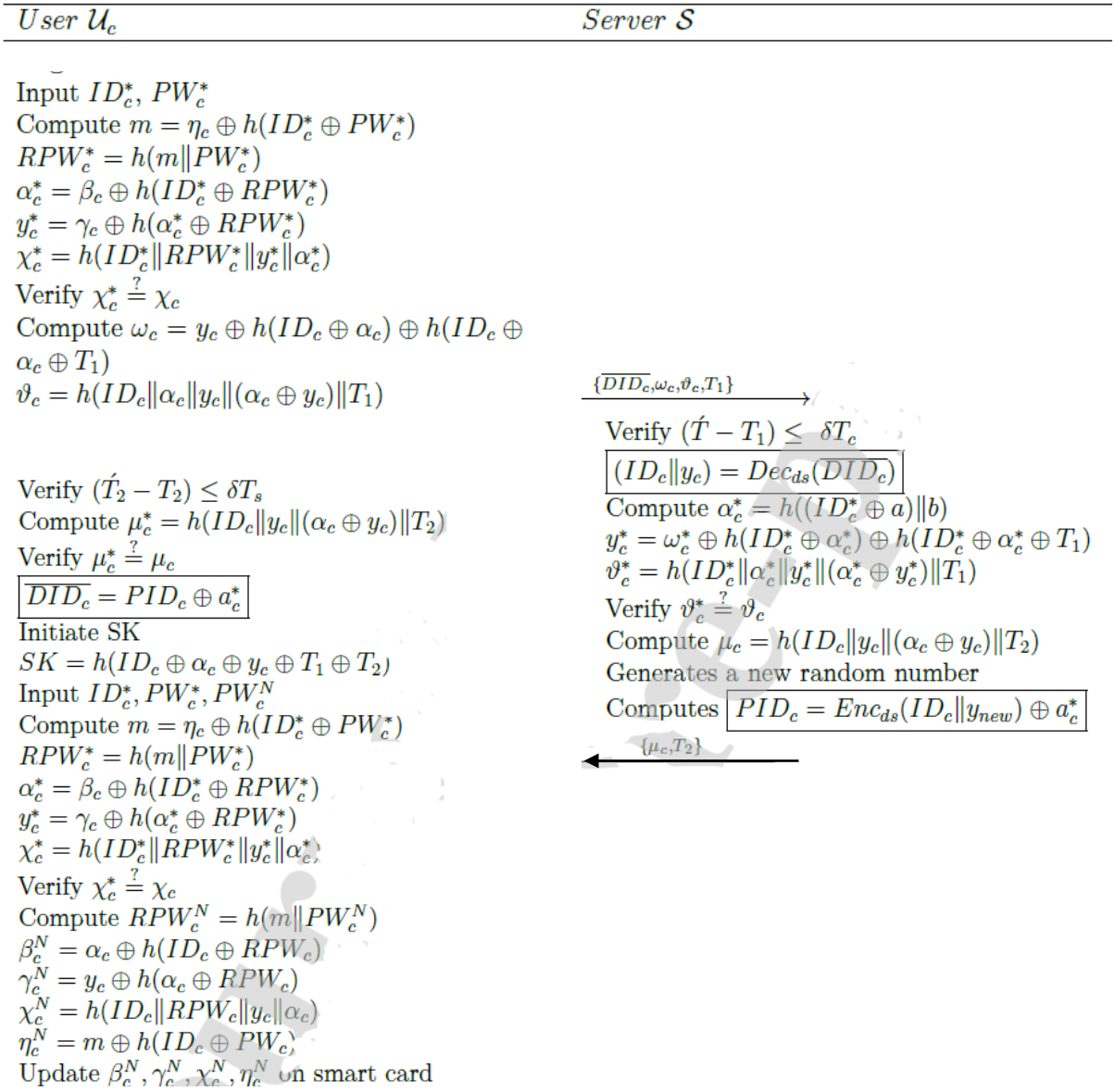
$$a_c^* = B_c \oplus h(ID_c^* \oplus RPW_c^*)$$
$$y_c^* = Y_c \oplus h(a_c^* \oplus RPW_c^*)$$

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.

$$RPW_c^N = h(m||PW_c^N)$$
$$B_c^N = a_c \oplus h(ID_c \oplus RPW_c)$$
$$Y_c^N = y_c \oplus h(a_c \oplus RPW_c)$$

$X_c^N = h(ID_c||RPW_c||y_c||a_c)$
$\eta_c = \mathrm{m} \oplus h(ID_C \oplus PW_c)$

درنهایت 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 می‌شود.




شکل ۱۹: مرحله ورود واحراز 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 الویت‌دار، به سرقت رفتن کارت هوشمند، حمله جعل‌کاربر و سرور، حمله حدس رمزعبور برخط/برون‌خط، 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 تحلیل های 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 قابلیت های محدود این محیط‌ها هم سازگار باشد ارائه نشده است. جدول ۸ خلاصه‌ای از آسیب‌پذیری‌های طرح‌های احرازاصالت 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

| طرح احرازاصالت | سال | ضعف امنیتی | طرح احرازاصالت بهبود یافته | سال |
|---|---|---|---|---|
| وینود و همکارانش [۱۵] | ۲۰۲۰ | حمله رله[1] و حمله جعل برچسب | صفخانی و همکارانش [۱۶] | ۲۰۲۱ |
| صفخانی و همکاران[۱۶] | ۲۰۲۱ | - | - | - |
| کومار و چوهان [۱۷] | ۲۰۲۱ | - | - | - |
| کومارپاندا و چپتاپدهی [۱۸] | ۲۰۲۰ | - | - | - |
| سونگاتی و همکاران [۱۹] | ۲۰۱۹ | - | - | - |
| مجمودر[2] و همکاران [۲۰] | ۲۰۲۱ | - | - | - |
| کال و آوستی [۲۱] | ۲۰۱۶ | حمله جعل هویت | طرح رانا و همکاران [۲۲] | ۲۰۲۱ |
| رانا و همکاران [۲۲] | ۲۰۲۱ | - | - | |
| شورسکومار و همکاران[۱] | ۲۰۱۹ | حمله نقض یکپارچگی، عدم ردیابی و غیر همزمان سازی | ECCbAS [۱۴] | ۲۰۲۳ |

## ۳-دلایل انجام طرح:

یکی از اهداف این پیشنهاد طرح تحقیقاتی 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، ذخیره سازی و ارتباطی در محدودیت هستند، انواع طرح های احراز اصالت ارائه شده است. تشخیص آسیب‌پذیری‌های موجود در این طرح‌های احرازاصالت 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 احرازاصالت در برابر طیف مختلفی از حملات بیشتر می شود 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 به‌دست 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 ذخیره سازی محدود این محیط‌ها

## ۵-برنامه و نحوهٔ اجرای طرح:

[1]-Relay attack
[2]-Majumder et al.

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 انجام‌خواهدشد.

- بررسی پیشینه تحقیق
- تحلیل امنیتی پروتکل‌های احرازاصالت ارائه شده برای محیط‌های با محدودیت منابع با استفاده از روش‌های غیرصوری و منطق‌های ریاضی مانندBAN ، GNY و مدل Real or Random Model (RoR)
- 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
- مقاوم‌نمودن 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-برنامهٔ 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 احرازاصالت ارائه شده برای محیط‌های با محدودیت منابع با استفاده از روش‌های غیرصوری و منطق‌های ریاضی مانندBAN ، GNY و مدل Real or Random Model (RoR) | 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 | ۱و۲ | ٪۲۰ | ۲ | | | | | | | | | | | | |
| ۴ | مقاوم‌نمودن پروتکل‌های احراز اصالت آسیب‌پذیر در برابر حملات و بررسی امنیت نسخه‌های بهبود یافته با استفاده از انواع روش‌های صوری، غیرصوری و انواع نرم افزارهای خودکار تحلیل امنیتی | ۲-۳ | ٪۳۰ | ۲ | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ۵ | مستند سازی و انتشار مقاله | ۴-۱ | ٪۳۰ | ۳ | | | | | | | | | | | | | | | | | |

## ۷-همکاران طرح:

- **دکتر معصومه صفخانی**: دکتری مهندسی الکترونیک- رمزنگاری، دانشیار گروه مهندسی نرم‌افزار دانشکده مهندسی کامپیوتر، دانشگاه تربیت دبیر شهید رجایی (https://scholar.google.com/citations?hl=en&user=C0CuSccAAAAJ&view_op=list_works&sortby=pubdate)
- دانشجویان تحت راهنمایی و تیم محققان همکار

## ۸-ابزار مورد نیاز:

- کامپیوتر پرسرعت برای مدلسازی، پیاده‌سازی و تحلیل امنیتی پروتکل‌های مختلف احراز اصالت برای محیط‌های با قابلیت‌های محاسباتی، ذخیره‌سازی، پردازشی و ارتباطی محدود

## ۹-بودجه بندی:

| ردیف | شرح هزینه | مبلغ ماهیانه (ریال) | تعداد ماه | جمع (میلیون ریال) |
|---|---|---|---|---|
| ۱ | دستمزد | ۲۰۰۰۰۰۰۰ | ۱۲ | ۲۴۰ |
| جمع کل (دویست و چهل میلیون ریال) | | | | ۲۴۰ |

## ۱۰-مراجع:


[1] Sureshkumar, V., Amin, R., Vijaykumar, V. R., & Sekar, S. R. (2019). Robust secure communication protocol for smart healthcare system with FPGA implementation. *Future Generation Computer Systems*, *100*, 938-951.

[2] Chanal, P.M. and Kakkasageri, M.S., 2020. Security and privacy in IoT: a survey. Wireless Personal Communications, 115(2), pp.1667-1693.

[3] Kumar, V., M. Ahmad, and A. Kumari, *A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS.* Telematics and Informatics, 2019. **38**: p. 100-117.

[4] Aslam, M.U., A. Derhab, K. Saleem, H. Abbas, M. Orgun, W. Iqbal, and B. Aslam, *A survey of authentication schemes in telecare medicine information systems.* Journal of medical systems, 2017. **41**(1): p. 14.

[5] Shi, X., J. Cao, T. Lu, and V. Chang. *A Survey on RFID Security and Privacy in Smart Medical: Threats and Protections*. in *IoTBDS*. 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.