Secure Web Based Home Automation

Application Layer Based Security Using Embedded Programmable Logic Controller

Gerfried Cebrat (*Author*)
Graz, Austria
gerfried.cebrat@chello.at

Abstract— **The paper postulates the feasibility of an open but secure and affordable home automation system. An Internet enabled embedded programmable logic controller is used in the context of intelligent networked Heating, Ventilation, & Air Conditioning (HVAC)-control. In the paper, security problems of the ecotope, comprising embedded controllers, web servers, and external services are analysed. In the absence of encryption of the channels, an application based security method was designed, preventing from simple manipulation of user data. Integrity of the intranet is secured via rigorous design, avoiding inbound traffic. A simplified sequence diagram documents this primary protection process, using rolling code encryption of the transmitted data. The security method was demonstrated successfully using an IP enabled universal industrial controller. Apart from security, process capability is investigated, analysing energy supply, communication channel options, bandwidth and real time requirements. Finalising, semantic enhanced, representational state transfer (REST), and resource definition framework are bespoken for the context of embedded.**

Keywords— HVAC, home automation, security, embedded controller, IoT

I. Applications and Requirements

A. Starting Point

Equipping newly built HVAC systems and retrofitting existing HVAC systems with intelligence supports remote information of users and remote control by the users, but also use of Open Data stemming from the Internet enabled devices. Additional data and networking will allow autonomous optimization of HVAC-operation and shall reduce energy demand. The presented approach is a counterpart to other appliances which are using data traces from citizens' behaviour implementing a service. We propose a user centric open but highly secure and network of appliances and services enabling energy and resource saving in homes. Open data shall benefit the process, since information about ambient conditions, mainly weather information, allows predictive control of the HVAC appliances. However, most important the system architecture shall respect private data and implement security measurers protecting from hijacking of the HVAC appliances or from data leakages. Securing user attendance data is most critical, since it may trigger burgling. It is to be proven that using a cost efficient programmable internet enabled controller may satisfy the requirements even in the absence of sufficient encryption capability.

B. Applications

Embedded controllers allow using algorithms, improving process quality of HVAC systems, reducing their energy demand. On top of that using information from users allows adapting the load curve, so it fits demand and reduces further the end energy demand. Finally yet importantly, open accessible weather information allows predictive control increasing the efficiency even further. Interfaces allowing the users adapting their preferences via the Internet may benefit acceptance of automation solutions. The following table lists archetypical applications and HVAC components in small offices and home office environments SOHO and denotes the potential energy savings:

TABLE I. Potential Applications Saving energy

Application	Savings by
Domestic Hot Water Supply	Minimizing of average water temperature over time by late and demand controlled heating.
Room Heating	Heat recovery from exhaust air
	Adding prediction from room and ambient temperature measurements avoiding temperature overshooting
	Adding presence sensors combining with historic data
	Predictive control of solar gains
	Feedback of room temperature towards user
	Detecting energy losses (open windows…)
Domestic Appliances	Feedback of energy demand towards the users
	Regulating start times depending on solar yield
	Detecting standby losses
Office Appliances	Feedback of energy demand towards the users
	Detecting standby losses
	Timer control of appliances/mains adaptors

For table I, automated switching of lights was not included because of the instant visibility of enabled lights and the low energy demand of state of the art illumination using Light Emitting Diode (LED) technology.

The attempt of rolling out energy saving solutions utilizing the Internet of things, at the same time challenging existing business models and market competitors, as installation bus based original equipment manufacturers (OEM) backed solutions or Radio Frequency (RF) based do-it-yoursef (DIY) automation is somewhat fragile. However, initiatives like the Nest project "Smoke and Carbon Monoxide Alarm" [5] shows that technology is ready to implement new networked solutions, and investors believe in the approach.

The first question for setting up a distributed control system is the availability of electric energy for the control devices. Existing central room thermostats are connected via 24V wiring and replacing IP-enabled controllers may be harvesting energy from this source. For electric heating elements in domestic hot water (DHW) appliances, there is 230V power

978-1-4799-3580-2/14/$31.00 ©2014 IEEE

available at least part of the night and electrolytic double layer capacitors (EDLC) might be used (possibly in future Lithium Ion Capacitors) storing energy for listening to commands during the day respectively the device will be polling the server infrequently for changes in the time schedule or user preferences. Other appliances are connected to 230V plugs and thus have ample energy available. So networking of the applications listed in table I seems to be feasible.

This leaves open the communication method for networking as second question. SOHO standards may be either wireless IEEE 802.11 or power line communication, integrating into Ethernet IEEE 802.3. In addition, gateways integrating IEEE 802.15.4, or home automation buses are available, but unfortunately at a price. Only very basic and simple technology like RF/X1 is cost efficient but not fulfilling our requirements concerning an open, but performing and secure controller ecotope.

Regarding triggers for actions in home automation, apps in nomadic devices are a means, also Location Based Services (LBS) using global navigation satellite systems (GNSS) like GPS have stepped in, however at the price of using external commercial services. If the time travelled from office to sufficient arrival prediction is helpful [6][7]. LBS may be also embedded in the vehicle as shown for vehicle to grid (V2G) approaches, but vehicle integrated solutions remain impracticable if different mobility (car, bicycle, public transport etc.) means are chosen on a trip-by-trip basis. For short commutes and heavy buildings, user based data input of planned return times is more effective.

C. *General Requirements*

Hardware and software paradigms for embedded controllers (connecting users and the Internet of Things IoT [2]) have to be harmonised in order to create critical mass. The system architecture shall generate an ecotope, allowing as much practitioners to participate to allow spread. Open system architecture is therefore essential, as well as protection of the source code written creating valid business models. Figure 1 depicts the basic requirements:

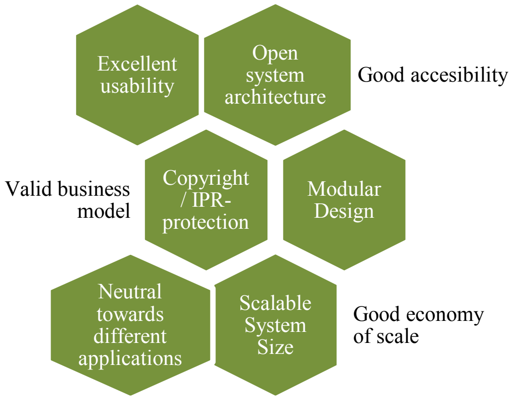


Figure 1 Requirements for success of a new automation paradigm

The following table II details the requirements concerning business model support, technology and user:

TABLE II. REQUIREMENTS FOR A NEW AUTOMATION SYSTEM

Supporting the innovative Business Model
- Remote software update capability
- High level programming languages, automated testing
- Secured intellectual property (access to plain control software code)
- Vivid piggy back module ecotope for sensors and actors
- Replication capability in production, swift setup for quick deployment
- Gateways to automation bus systems
Technological excellence
- Low energy demand (deep sleep, buck converter for voltage supply)
- High mean time between failure MTBF
- Low mean time to repair MTTR
- Scalable extensible system architecture
- Stable communication stacks
- Plug and Play Capability, integrating into SOHO networks
High User Acceptance
- Privacy protection of user data and status
- High intrusion security protecting intended device status
- Small size for easy integration of controllers
- EMC electro magnetical compatibility, especially radiation control
- Low noise (no fans, only solid state relay)

Especially remote software update is not trivial, if the devices are behind firewalls, device triggered updates shall be controllable a reroll able by the user avoiding damages.

D. *Security issues*

HTTPS is not supported by some embedded web enabled controllers; the required safe hash algorithms SHA-3 is not widely available yet. Even if implementing SSL on 8-bit microcomputers is possible [9], beginning transition to 32-bit systems greatly eases the use of encryption, providing standard libraries also for embedded clients. In the last time, more developments have taken up the problem and improved security for embedded devices [13]. Storing keys in trusted platform modules TPM is not regarded secure, the use of security boxes is favored [14] storing master keys in non-addressable memory (hardware). The introduction of HTTPS will lead to increased power consumption, because of the encryption and longer transmission times caused by the encryption overhead. A general problem might be WLAN networks in case more of more aggressive attacks.

II. Selection of Technological Solution

A. *Communication technologies and energy supply for operation*

In the following table III, the usability of power line and wireless communication are investigated for the various applications, as well as envisaged energy supply.

TABLE III. SUITABILITY OF COMMUNICATION TECHNOLOGIES AND ENERGY SUPPLY FOR APPLICATIONS

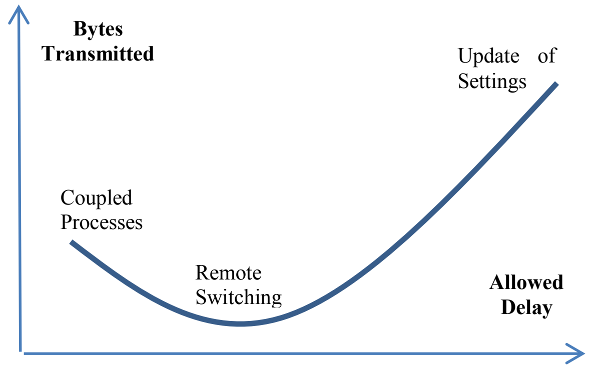
Application	**Power Line Comm.**	**Wireless attenuation**	**Energy supply**
Domestic Hot Water Tanks	Yes	Higher for cellars	Interrupted power supply
Kitchen water heater	Yes	Low	Power Grid
Home thermostats	No	Low	24V
White Goods Control	Yes	higher for cellars	not necessary
Window Status	No	Higher for cellars	Energy harvesting or batteries
Door Status	No	Higher outer doors or cellars	Difficult for inner doors
Room thermostats	No	Higher for cellars	Energy harvesting or batteries
Automated Shading	Yes	Low	Power Grid
Outlet switching	Yes	Higher for cellars	Power Grid
Illumination	Yes	Higher for cellars	Power Grid

From table III one may deduct that Power Line Communication is not suited for covering all applications, wireless communication may face attenuation problems in remote areas of the house. Energy supply is most difficult for single thermostats and doors inside the house leaving only few alternatives.

B. *Performance*

Performance requirements differ for the type of application. Fig. 1shows potential problems for closely coupled processes like shading control using remote light sensors arrays, where update intervals should be low and transmitted data amount might be significant. General HVAC-processes however listed in table II do not pose problems concerning bandwidth or delay limitations.

Fig. 1. Requirements for bandwidth and round trip time



Because of the absence of real time requirements, for tactic control of HVAC systems, and for energy storing devices, a server-based control is feasible, where embedded controllers acquire control data from servers. For shading control, using illumination sensor arrays, decentralized control systems using intelligent controllers are needed, because of the round trip times of the IP-based system.

III. PROPOSED SYSTEM DESIGN

A. *Overview*

The proposed system is storing user preferences and user input, which is transmitted via HTML forms or applets, using trusted web services. The embedded microcontrollers are addressing those web services to retrieve data and may query other controllers within the Intranet, or add data via the Internet if declared Open Data by the owners, using the same way, addressing the respective servers.

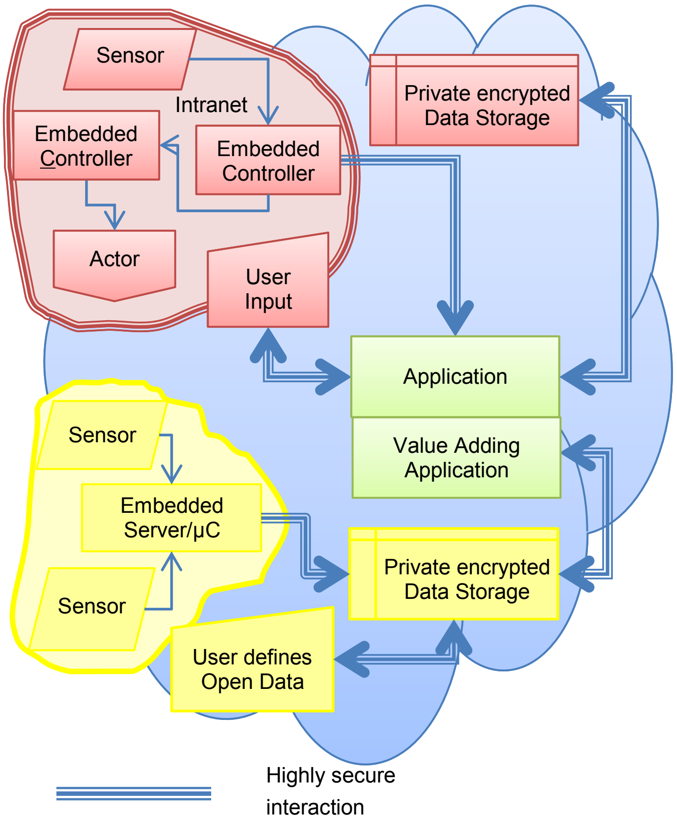


Figure 2 System's functions blocks, users connected via Internet

The communication between the controllers is within the Intranet, protected by a firewall, and closed ports on the router. This way the internal communication might be regarded sufficiently secure if LAN/WLAN routers are well secured. For controlling the system from abroad, an incoming data flow is needed. Because the firewall should not be penetrated; data is transmitted back to the controller if the controller calls server scripts uploading controller data via GET. The status and preferences data is stored on the secure (external) server. This data may be entered via HTML-forms or via apps but also amended by Open Data preferably following OpenIoT standards [15]. Transmission of the HTML form data shall use transport layer security (SSL).

B. *Security Assessment*

Status files for HVAC might be altered, if the aggressor gets access right to the server. If this is the case also, the PHP files processing the GET calls are involved and the whole system is out of control. By all means, encryption of the transmission of status and preferences data files will be used obscuring this sensitive data. Since the controller calls the server retrieving data, the intrusion might be initiated via man in the middle attack. This way the aggressor might replace the return path of the GET call to the server. The consequences however vary for the different services. Leaked data, insertion of fake data, and interruption of the service should be prevented. The status for HVAC equipment is slowly changing only several times a day. The status is queried frequently from server by the microcontrollers having the chance to correct malicious settings. Table IV summarizes potential consequences of hacking the system for the different processes.

TABLE IV. WORST CASE CONSEQUENCES FOR INFLICTED PROCESSES

Process	Potential Consequences
µC sends Data to server for logging	Data unusable, or lost, or leaked
User sets HVAC Status/Preferences via HTML-form	Disrupted operation Extreme operation conditions Works in default mode Attendance or preferences Data leakage
HVAC gets data Status/Preference data from Server	
Server retrieves forecast	Wrong operation logic Using Default data

C. Specifying a Secure Design

A secure system needs authentication and identity security, according to the Carl Ellisons authentication triangle [3]. Fig. 4 analyses all criteria for secure systems for those criteria.

Fig. 2.

Process	Authentication	Confidentiality	Integrity	Availability
µC sends Data to server for logging	Via static IP-address	Transport layer protection	Checksum	Notify user if interrupted
User sets HVAC Status/Preferences via HTML-form	Password protection + Transport layer security	Transport layer protection	n/a	Acknowledgement from server
HVAC gets data Status/Preference data from Server	Via static IP-address	Transport layer protection	Checksum	Notify user if not accessible
Server retrieves forecast	Transport layer security	Transport layer protection	Integgrity check	Notify user if broken (via µC)

Figure 3 Assessment of the processes' security used in the system architecture (checklist from [4])Assessment of the processes' security used in the system architecture (checklist from [4])

Working though this list - introducing security measures - the remaining risk is regarded as being low if the wireless access is secured. The calls from the controller to the server are using fixed IP-addresses. Solely private encryption keys may add authenticity indirectly. The controllers are password protected and there is no inward port open on the router connecting the controllers to the internet. Absence of encrypted communication between server and controller should be fixed with an intermediate approach. The protection scheme is using rolling keys at the server and the controller. Those keys are secret to the point, that the PHP code including the keys has to be transmitted via FTP to the server. Keys are encrypted via PHP and stored on the server. The controller calls the server in our protective scheme as shown in Fig. 6. The returned value to the controller is modified using the key known to the receiver. Since programmable logic controllers do offer bit shifting and other basic algebra, simple en- and decryption of data transmitted is possible. Elliptic curves to be used as acclaimed method are possibly outside the scope with ladder logic programmable devices, if root functions are not offered.

Additional security may be introduced adding protective logic to the embedded controller. Checking plausibility of target temperature of HVAC appliances is easy, limiting room temperatures to feasible values, but checking integrity of attendance status via logic is very difficult if no user tracking is involved. However, if the status is read from the server in regular intervals using a rolling key for encryption, then exploitation of a hack is limited to the interval the key changes automatically and invisibly for the man in the middle. The data stored on the server might be checked by the user via HTML status form or App from abroad. Systems may never be designed completely bullet proof, but damages claimed by media if networked HVAC is hacked may be reduced, if the system is hardened in the described way and if protected logic in the embedded devices is limiting user settings to plausible values.

Finally, the user is send a status update if deviations are detected or a service is interrupted. If notification is done via secured email channel or better SMS adding an alternative second channel, then the system is even better protected. Changing the controller's program from remote may be prevented if the code may not be readable at all. Replacing the program needs knowledge about the wiring to be able addressing specific relays causing more harm. In the worst case, the HVAC devices are shut down if the program is deleted. Intrusion protection is the last and most important protection, because notification of users and plausibility check might be prevented by altering the controller program. If a good and not compromised firewall, using stateful inspection is used and a strong password for local programming of the controller, then risks are reduced to an acceptable level.

The shown example features a solution which may be realised using state of the art Programmable Logic Controllers PLC technology as for example CAINetworks WebControl™ Universal Industrial Controller [1]. The solution will work in existing SOHO environments, using Ethernet switches, and routers for connecting to the wide area network (WAN).

IV. FINDINGS AND OUTLOOK

A. Technical Findings and Outlook

The communication using GET over HTML-protocol was tested in a SOHO environment, showing round trip times below 100ms [10] supporting feasibility of the approach. In addition, it has been validated in practice that jitter does not harm syncing intervals of collaborating controllers for heat recovering cycling venting.

The application uses external data only for setting targets, so real time issues do not appear. The long round circle communication time of IP enabled controllers using GET to transport data needed modifications in shading control being near real time. In order to avoid instability, projections of the movements of the shading devices had to be used. For DHW and room thermostats and on/off control however this is not relevant as the processes including room temperatures have high damping rates and do not require real time features of the controlling system.

Test operation has shown some dropouts in the communication between embedded Internet enabled microcontroller and the server. This fact does not harm automation within the intranet but cuts of from remote control via the internet. To avoid unnecessary energy consumption in case of appliances settings fallback to default mode, local intelligence including attendance sensor have to be added. A watchdog, restarting the embedded Internet enabled microcontroller, will resolve most of the issues on the local side, clearing blocked communication stacks and rereading sensor codes. For the availability of the Internet server side, the provider choice is essential. Replication of the application on a second server, and more introducing a second communication WAN channel seems to be overshooting for HVAC applications, but with security control this is a must.

Security features of embedded IP-enable controllers shall be improved utilizing secure hash algorithms, also covering save firm- and software update. The solution using GET for data transmission may be seen as intermediate, modern embedded microcontrollers do feature communication sockets allowing methods that are more sophisticated without compromising the rigorous security oriented design.

Sending Declarative Sensor Interface Descriptors (DSID) to the web service registering new sensors allows integrating more information for added services, if the data owner declares this data open. For keeping bandwidth low, semantic information transmitted with the measurements should refer to the DSID keeping the transmitted sensor data small, not using XML, but EXI (Efficient XML Interchange) or JSON.

B. Market outlook

IHS predicts a growth of home automation expenditures of 40% in 5 years [8]. It is rather likely that the potential will be implemented not only using existing installing bus systems but also will access SOHO technologies namely using the internet protocol for economic reasons. However, it remains open, whether a critical mass is available, or the markets will remain divided into several segments using different physical communication layers. High volume security controllers for the automotive industry [14] might be adapted for home automation. Using less stringent requirements concerning transmission rate and ambient condition may lower prices.

Energy saving microcontrollers are beginning to use standard 32-bit CPU-technology, introducing high-level languages and comfortable integrated developing environments. While for prototyping controllers development boards are helpful including AD and 1wire interfaces and ladder logic, heading to production criteria change towards long uptime, easy cloning of controllers and remote code update, while protecting code at the users' premises. Those new 32-bit systems allow a connection to a variety of bus topologies so rolling out home automation will be eased.

The presented open system architecture allows others to step in if the interfaces are public. Commercial services might provide local weather forecasts but also thermography data or offer application program interfaces. The unique selling proposition lies in the quality of the algorithms. External - may be ad-financed services - may serve as portal for linking on-line calendars with weather forecast and home automation merging user interfaces. However, data security is not compromised if calendar data is hosted on the client's server. The open system architecture will allow further collaboration models between neighbours, depending on physical (piping) and legal (power selling licence) boundaries.

REFERENCES

[1] http://www.cainetworks.com/products/webcontrol/index.html

[2] William J. Miller, Intrusion Prevention for Sensor Networks, M2M & the Internet of Things (IoT)

[3] Sumeet Singh; SecureWS - A Secure, Application Layer Communication Channel for Web Services;

[4] Dan Wendlandt; Secure Communication with an Insecure Internet Infrastructure, Lecture

[5] Q. Hardy, "Nest's Tony Fadell on Smart Objects, and the Singularity of Innovation One on One November 7, 2013, 21:00

[6] Gupta M., Intille S., Larson K., „Adding GPS-Control to Traditional Thermostats: An Exploration of Potential Energy Savings and Design Challenges; 2009

[7] Scott J., et al.; Home Heating Using GPS-Based Arrival Prediction; 2010

[8] S. Riaz, US building automation systems market will reach USD 1.65 bn by year-end: HIS" 12 Nov 13; Insights Intelligent Building Today

[9] Stapko Timothy; Implementing SSL on 8-bit micros, 2004 http://www.embedded.com/design/prototyping-and-development/4006433/Implementing-SSL-on-8-bit-micros

[10] Anonymous, Final report of the Anonymous project 2010

[11] Kleidermacher, D.; Security Considerations for Embedded Operating Systems, Green Hills Software, Inc. June 8, 2006 http://www.embedded.com/design/operating-systems/4006664/Security-Considerations-for-Embedded-Operating-Systems

[12] Guy S. A., US Patent Application 20130246800 Enhancing Security of Sensor Data for a System Via an Embedded Controller, Microchip Technology Incorporated

[13] Greenfield D., Security Gets Embedded", AutomationWorld Embedded Control January 8, 2013

[14] Bogdanov A., Carluccio D., Weimerskirch A., Wollinge T., Embedded Security Solutions for Automotive Applications, published in Valldorf, Gessner W. (Eds.) Advanced Microsystems for Automotive Applications 2007, Springer Verlag, VDI Book, 2007

[15] Phillips Amya; Internet of Things to become a reality at ARM Headquarters, 25.07.2013; ARM Connected Community and http://wiki.1248.io/doku.php

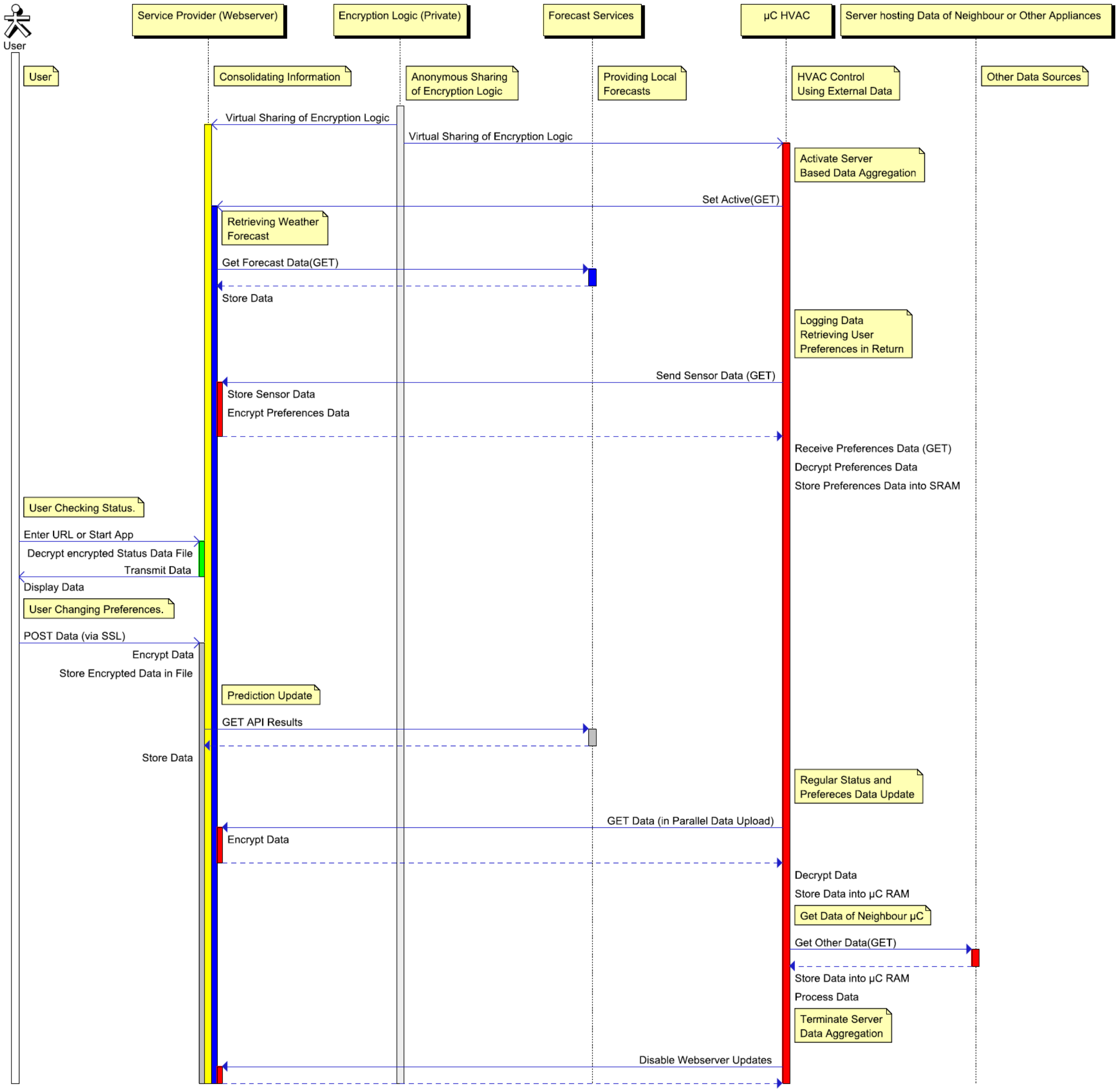

User
Service Provider (Webserver)
Encryption Logic (Private)
Forecast Services
µC HVAC
Server hosting Data of Neighbour or Other Appliances
User
Consolidating Information
Anonymous Sharing of Encryption Logic
Providing Local Forecasts
HVAC Control Using External Data
Other Data Sources
Virtual Sharing of Encryption Logic
Virtual Sharing of Encryption Logic
Activate Server Based Data Aggregation
Set Active(GET)
Retrieving Weather Forecast
Get Forecast Data(GET)
Store Data
Logging Data Retrieving User Preferences in Return
Send Sensor Data (GET)
Store Sensor Data
Encrypt Preferences Data
Receive Preferences Data (GET)
Decrypt Preferences Data
Store Preferences Data into SRAM
User Checking Status.
Enter URL or Start App
Decrypt encrypted Status Data File
Transmit Data
Display Data
User Changing Preferences.
POST Data (via SSL)
Encrypt Data
Store Encrypted Data in File
Prediction Update
GET API Results
Store Data
Regular Status and Prefereces Data Update
GET Data (in Parallel Data Upload)
Encrypt Data
Decrypt Data
Store Data into µC RAM
Get Data of Neighbour µC
Get Other Data(GET)
Store Data into µC RAM
Process Data
Terminate Server Data Aggregation
Disable Webserver Updates

Figure 4 Sequence diagram of the communication showing the securiy approach (Strauch: Quick Sequence Diagram Editor)

978-1-4799-3580-2/14/$31.00 ©2014 IEEE