Signature-Based Authentication in Future Internet of Things (IoT) Applications

Dr. Ashok Kumar Das

IEEE Senior Member
Associate Professor
Center for Security, Theory and Algorithmic Research
(Department of Computer Science and Engineering)
International Institute of Information Technology, Hyderabad
(Formerly **Indian Institute of Information Technology, Hyderabad**)

E-mail: *ashok.das@iiit.ac.in*
Homepage: http://www.iiit.ac.in/people/faculty/ashokkdas
Personal Homepage: https://sites.google.com/view/iitkgpakdas/

September 25, 2022

Internet of Things (IoT)

- A “thing” in the IoT can be a person, animal or physical/virtual object with a unique identifier (IP address or device ID) that has the ability to transfer data (sensing information from surrounding area) via the Internet.
  - *Physical object:* Smartphone, camera, sensor, vehicle, drone, etc.
- The “Things” in IoT usually referes to IoT devices. IoT devices can perform remote sensing, actuating (making an action), and monitoring capabilities.
- A thing can be smart and thus, the thing can make a decision without human’s help (intervention).
  Majority of things are expected to be smart in the future.
- The objective of IoT is to integrate computer-based systems and the physical world for economic benefit and to improve accuracy and efficiency while reducing human involvement.
- An estimated 50 billion objects will be a part of IoT by 2020.

Internet of Things (IoT)

Table: IoT units installed based by category (millions of units)

Category	2016	2017	2018	2020
Consumer	3,963.00	5,244.30	7,036.30	12,863.00
Business: cross-industry	1,102.10	1,501	2,132.60	4,381.40
Business: vertical-specific	1,316.60	1,635.40	2,027.70	3,171
Grand total	6,381.80	8,380.60	11,196.60	20,415.40

Table: IoT endpoint spending by category (millions of dollars)

Category	2016	2017	2018	2020
Consumer	532,515	725,696	985,384	1,494,466
Business: cross-industry	212,069	280,059	372,989	567,659
Business: vertical-specific	634,921	683,817	736,543	863,662
Grand total	1379,505	1,689,572	2,094,881	2,925,787

Ref. Information Matters. The Business of Data and the Internet of Things (IoT). http://informationmatters.net/internet-of-things-statistics/. Accessed on August 2018.

Signature-Based Authentication in Future Internet of Things (IoT) Applications

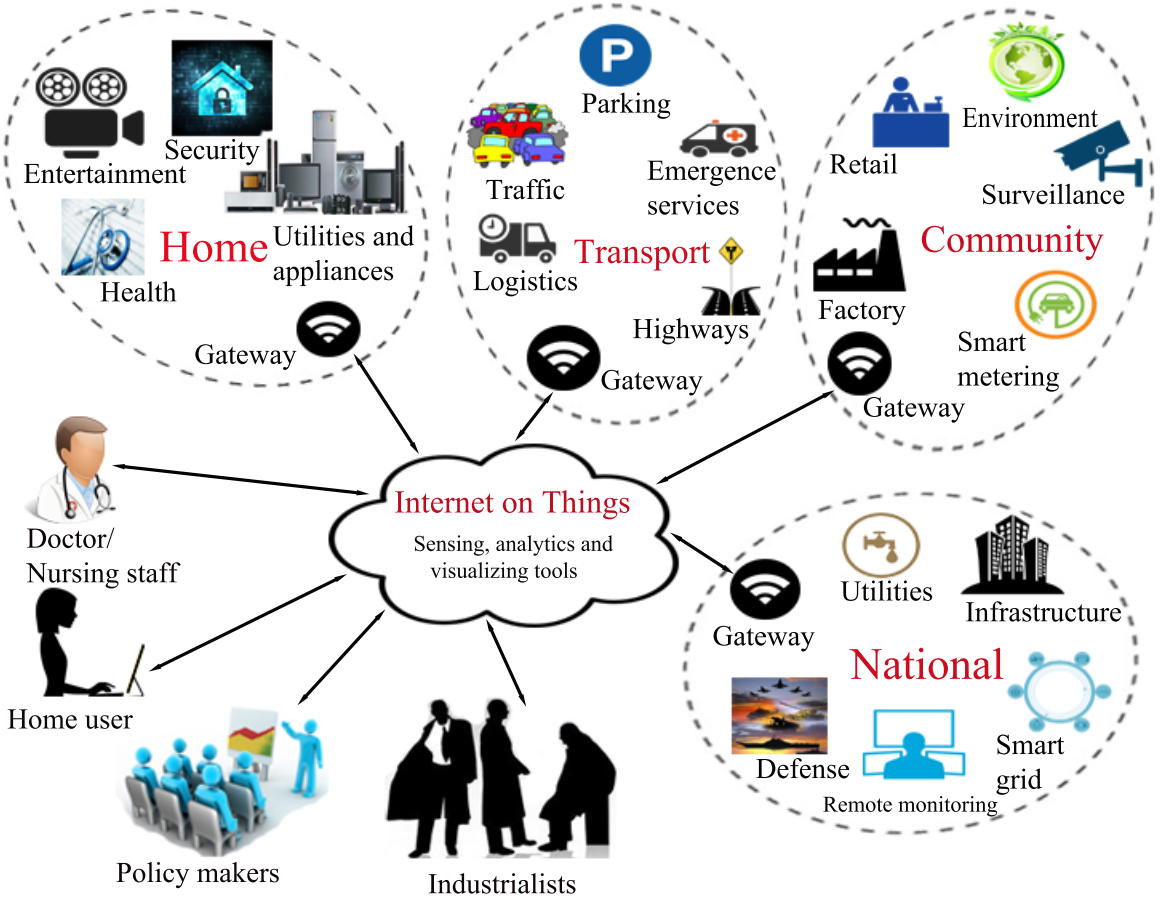
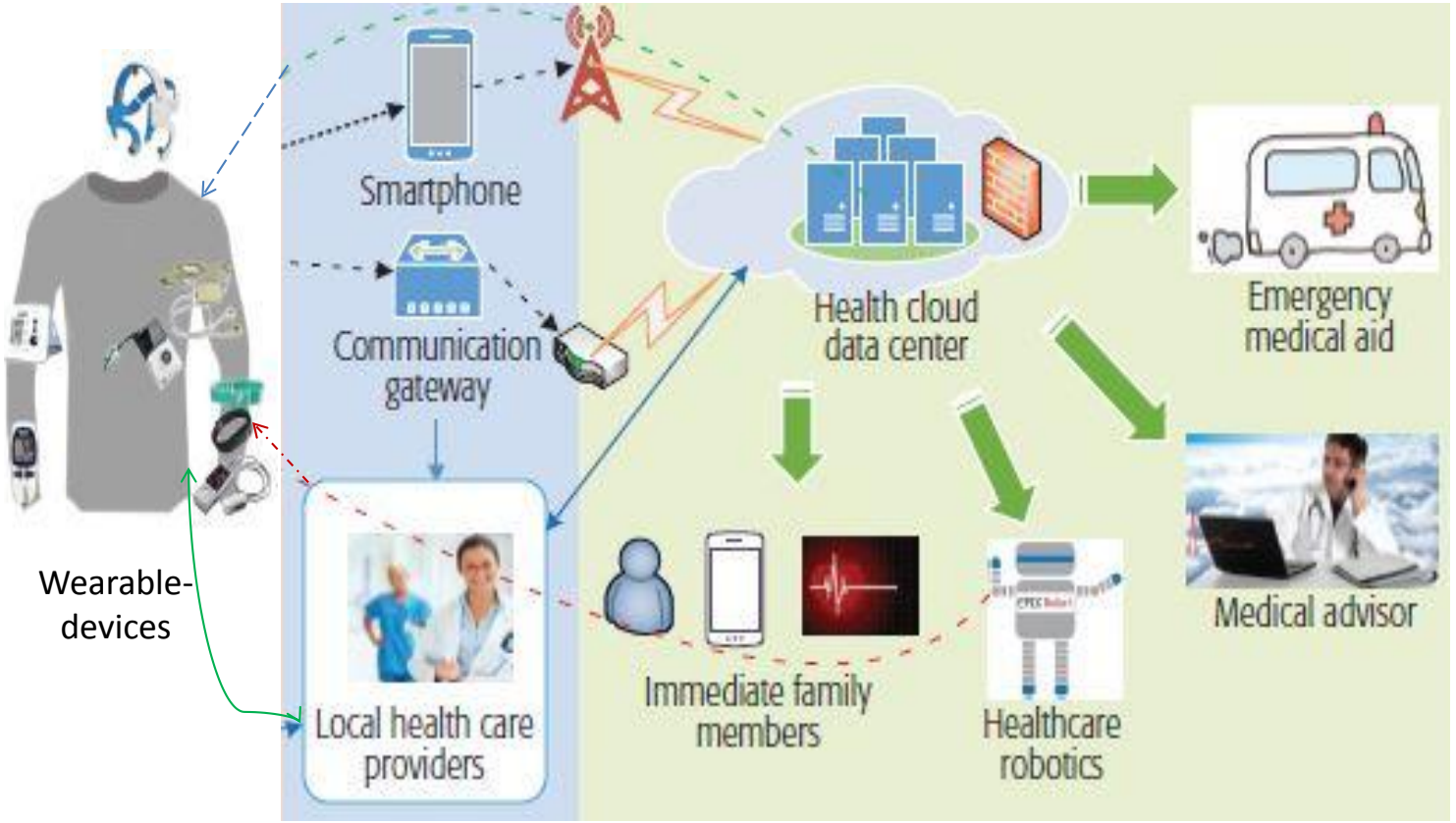


Figure: IoT authentication model

IoT authentication model

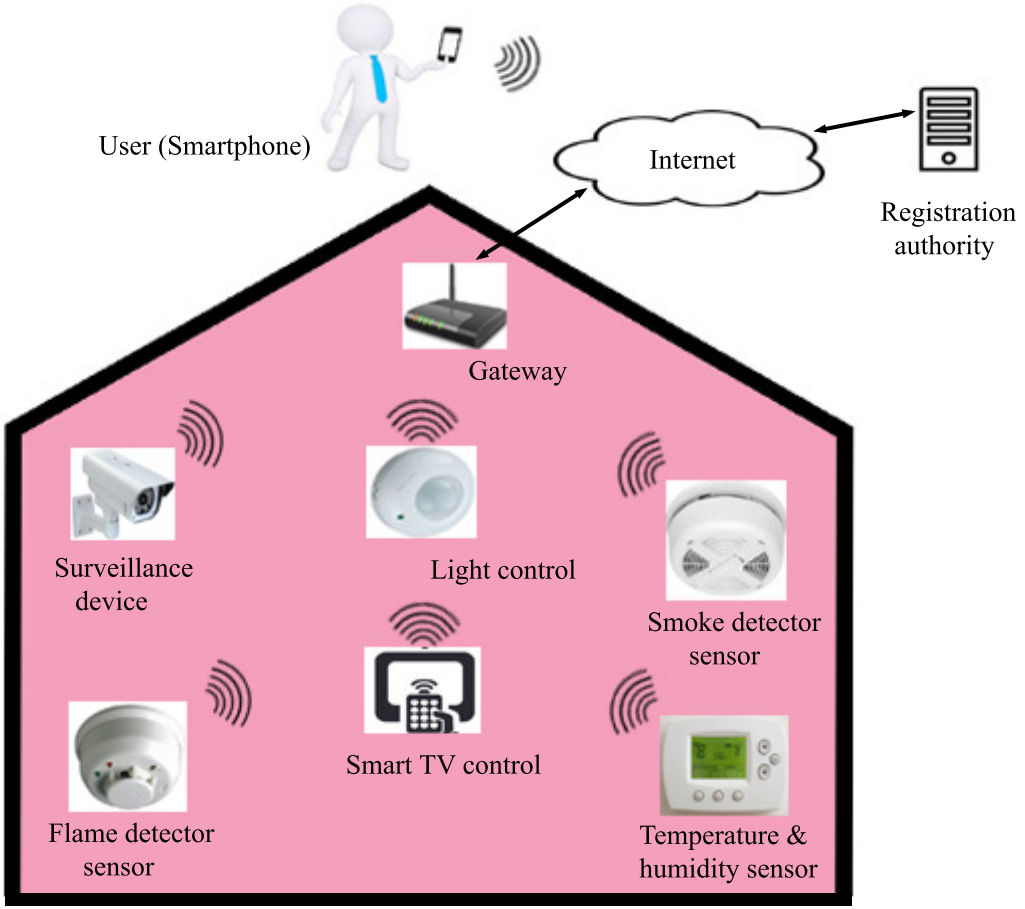
- IoT authentication model considers four different scenarios, i.e., Home, Transport, Community and National.
- All these scenarios have smart devices, such as sensors and actuators, which facilitate the day to day life of people.
- In the given scenarios, all smart devices are connected to the Internet through the gateway nodes (*GWN*s).
- Different types of users (for example, smart home user and doctor) can access the data of relevant IoT devices through the *GWN*.
- Mutual authentication between a user and a device through the *GWN* provides access to device data to the user.

IoT Applications: Healthcare



Jangirala Srinivas, Ashok Kumar Das, Neeraj Kumar, and Joel J. P. C. Rodrigues. "Cloud Centric Authentication for Wearable Healthcare Monitoring System," in **IEEE Transactions on Dependable and Secure Computing**, Vol. 17, No. 5, pp. 942-956, September/October 2020, DOI: 10.1109/TDSC.2018.2828306.

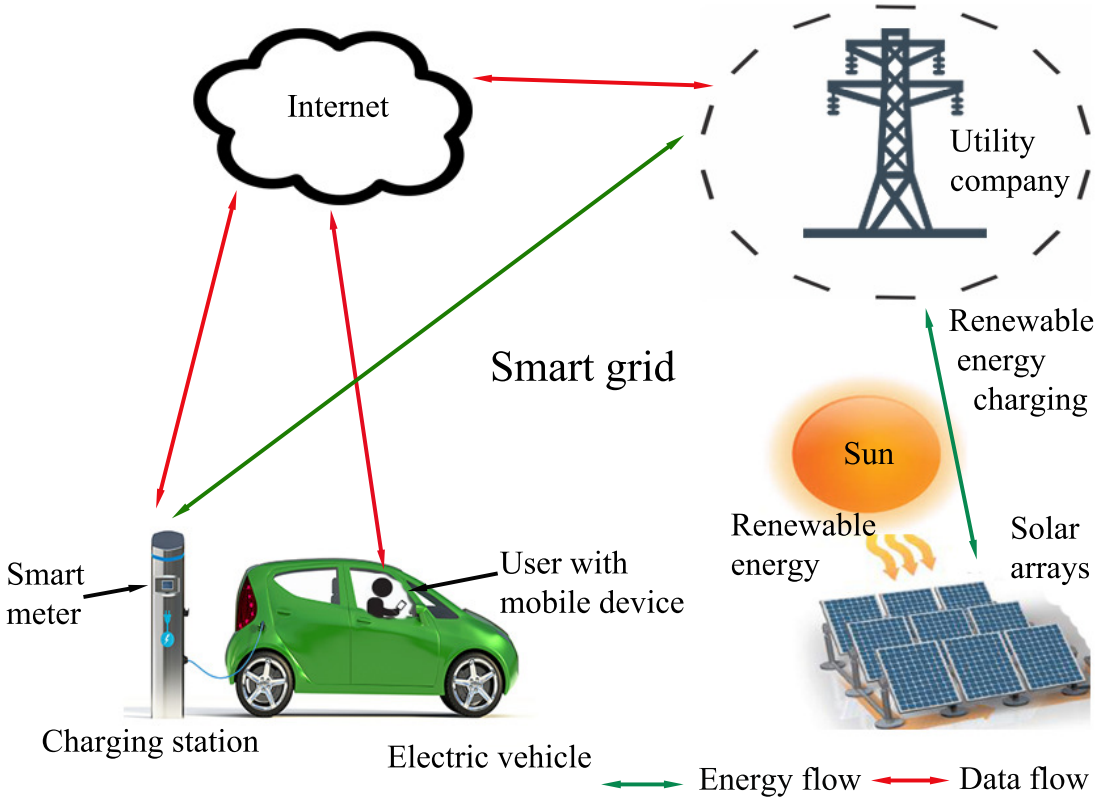
IoT Applications: Smart Home



Smart Home

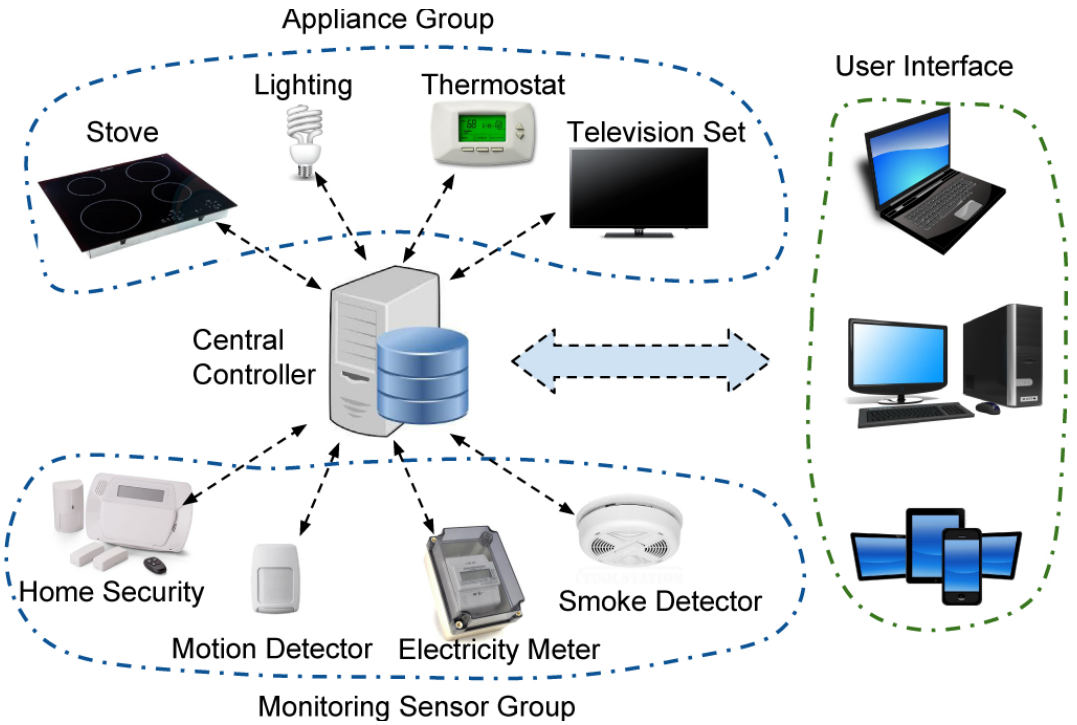
Mohammad Wazid, Ashok Kumar Das, Vanga Odelu, Neeraj Kumar, and Willy Susilo. "Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment," in **IEEE Transactions on Dependable and Secure Computing**, Vol. 17, No. 2, pp. 391-406, 2020, DOI: 10.1109/TDSC.2017.2764083.

IoT Applications: Renewable Energy-Based Smart Grid



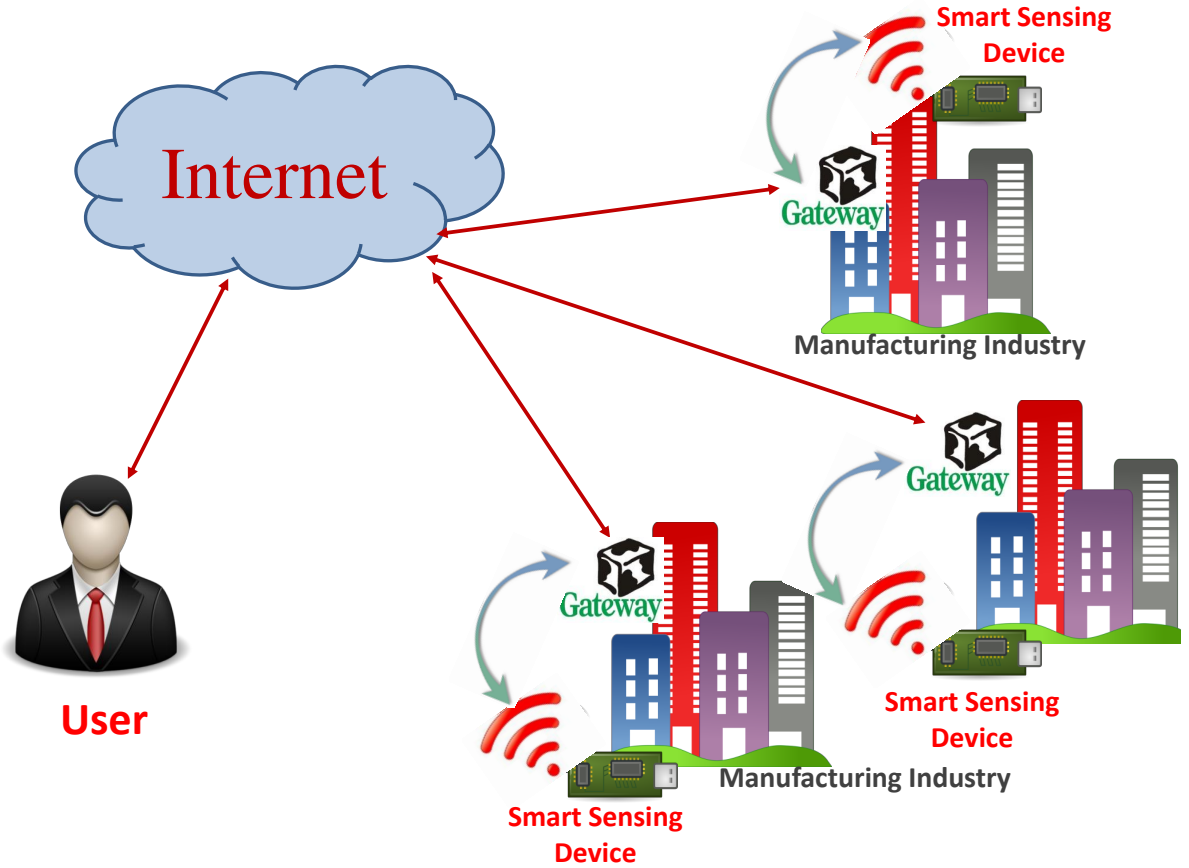
Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, and Joel J. P. C. Rodrigues. "Secure Three-factor User Authentication Scheme for Renewable Energy Based Smart Grid Environment," in **IEEE Transactions on Industrial Informatics**, Vol. 13, No. 6, pp. 3144-3153, 2017, DOI: 10.1109/TII.2017.2732999.

IoT Applications: Smart Home



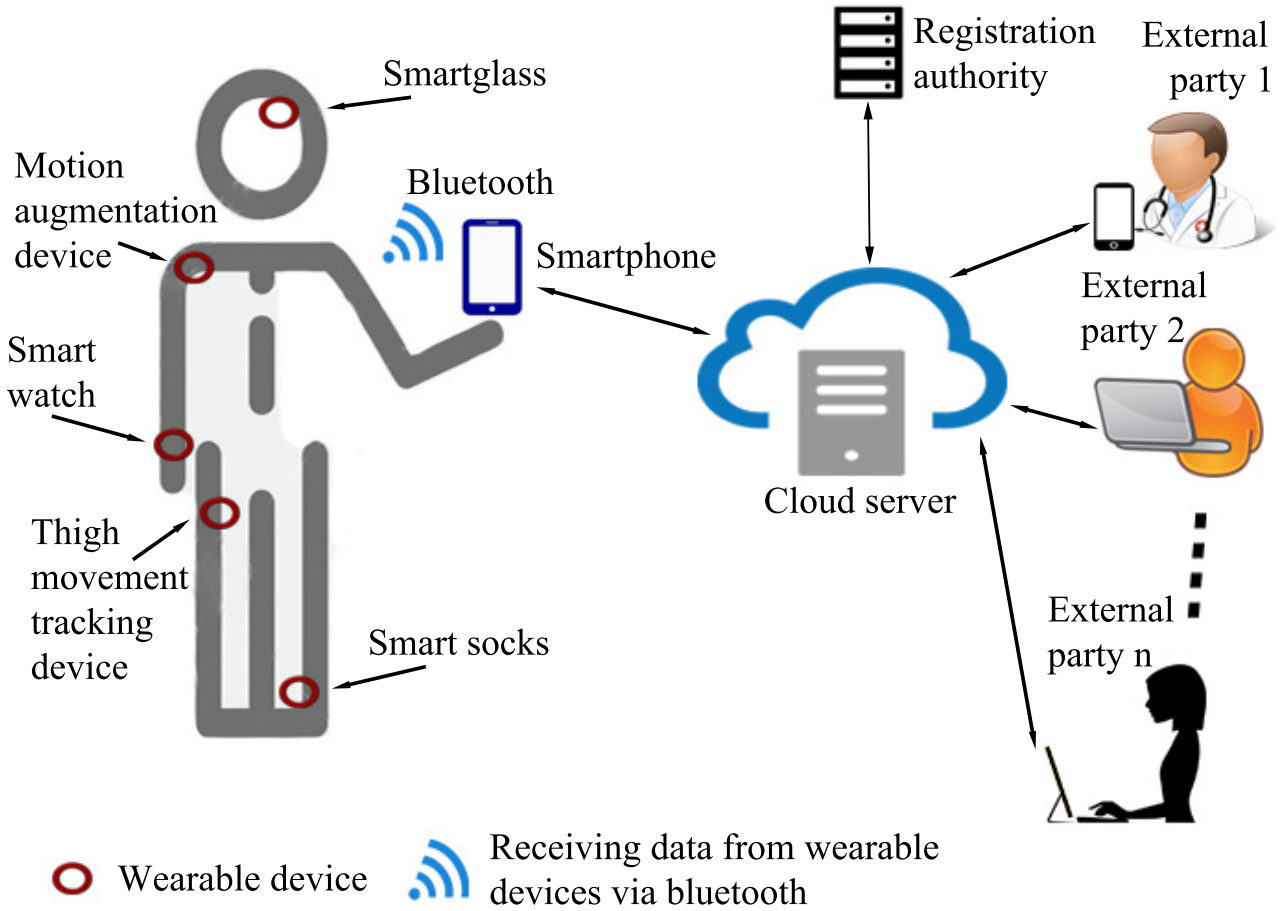
Mohammad Wazid, Ashok Kumar Das, Vanga Odelu, Neeraj Kumar, Mauro Conti, and Minho Jo. "Design of Secure User Authenticated Key Management Protocol for Generic IoT Network," in *IEEE Internet of Things Journal*, Vol. 5, No. 1, pp. 269-282, 2018.

IoT Applications: Industrial IoT



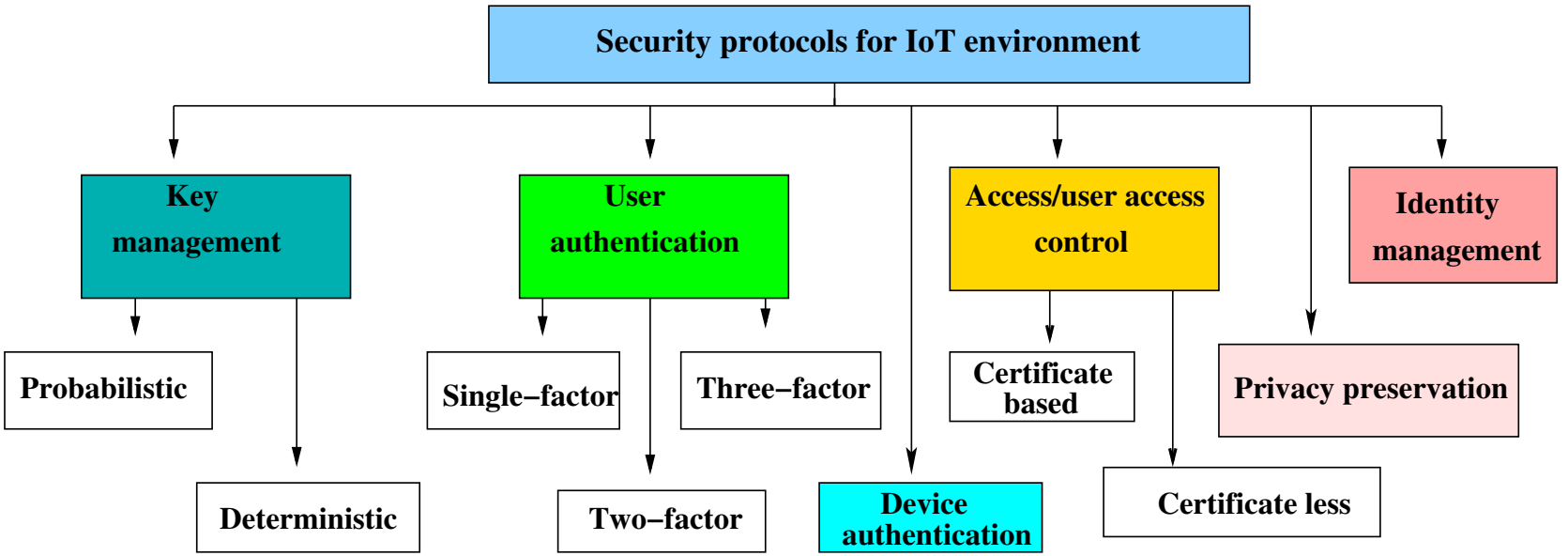
Jangirala Srinivas, Ashok Kumar Das, Mohammad Wazid, and Neeraj Kumar. "Anonymous Lightweight Chaotic Map-Based Authenticated Key Agreement Protocol for Industrial Internet of Things," in *IEEE Transactions on Dependable and Secure Computing*, ol. 17, No. 6, pp. 1133-1146, 2020, DOI: 10.1109/TDSC.2018.2857811.

IoT Applications: Healthcare



Ashok Kumar Das, Mohammad Wazid, Neeraj Kumar, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, and YoungHo Park. "Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment," in **IEEE Journal of Biomedical and Health Informatics (Formerly, IEEE Transactions on Information Technology in Biomedicine)**, Vol. 22, No. 4, pp. 1310-1322, 2018.

Taxonomy of security protocols in IoT



Ashok Kumar Das, Sherali Zeadally, and Debiao He. "Taxonomy and Analysis of Security Protocols for Internet of Things," in *Future Generation Computer Systems (Elsevier)*, Vol. 89, pp. 110-125, 2018, DOI: 10.1016/j.future.2018.06.027.

Security requirements in IoT environment

- **Authentication:** It involves authentication of sensing devices, users and gateway nodes before allowing access to a restricted resource, or revealing crucial information.
- **Integrity:** The message or the entity under consideration must not be changed to ensure integrity.
- **Confidentiality:** Confidentiality or privacy of the wireless communication channel protects from the unauthorized disclosure of information.
- **Availability:** The relevant network services should be made available to authorized users even under denial-of-service attacks on the system.
- **Non-repudiation:** It aims to prevent a mischievous entity from hiding his/her actions.
- **Authorization:** It confirms that only the legitimate IoT sensing (smart) devices can supply information to network services.
- **Freshness:** It confirms that the information is fresh and the old messages cannot be replayed by any adversary.
- Apart from the above security requirements, the following two important security properties should also be satisfied:
  - **Forward secrecy:** If an IoT sensing node quits the network, any future messages after its exit must be prohibited.
  - **Backward secrecy:** If a new IoT sensing node is added in the network, it must not read any previously transmitted message.

Security attacks in IoT environment

- **Replay attack:** A replay attack is one in which an adversary, $\mathcal{A}$ attempts to mislead another authorized entity by reusing the information during the transmission.
- **Man-in-the-middle attack:** Under such an attack, $\mathcal{A}$ intercepts the transmitted messages and tries to change/delete/modify the contents of the messages delivered to the recipients.
- **Stolen-verifier attack:** This attack can occur if the *GWN* in the IoT network stores any verifier/password table for user/device verification. In such an attack, $\mathcal{A}$ can steal a user's credentials such as identity or password from the table.
- **Stolen/lost smart card attack:** If $\mathcal{A}$ has a lost/stolen smart card, he/she can extract all the credentials stored into its memory by using techniques such as power analysis attacks. Using the extracted information, $\mathcal{A}$ can then derive the secret credentials.
- **Password guessing attack:** In a password-based scheme, $\mathcal{A}$ may attempt to guess the password of a legal registered user either online or offline mode with the help of the eavesdropped messages and also stored credentials in the system or a user's smart card (mobile device).

Security attacks in IoT environment (Cont...)

- **Password change attack:** Under this attack, $\mathcal{A}$ may try to change the password of an authorized registered user.
- **Denial-of-Service attack:** A Denial-of-Service (DoS) attack is any event that prevents a system's or network' capability to perform its expected function.
- **Privileged-insider attack:** In this kind of attack, a trusted user within the organization (also known as an insider) can act as a privileged-insider attacker.
- **Impersonation attack:** In an impersonation attack, an attacker may attempt to falsify a fake message to defraud other recipient entities in a network on behalf of a sending entity.
- **Resilience against smart device physical capture attack:** In IoT environment, except the *GWN* the IoT sensing devices are not physically protected. Hence, there is a possibility of physical capturing of the sensing devices by an attacker $\mathcal{A}$. $\mathcal{A}$ can then use the extracted information stored in those captured sensing devices to compromise communication between other non-compromised sensing devices.

Signature-Based Authentication in Future Internet of Things (IoT) Applications

- Sravani Challa, Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Alavalapati Goutham Reddy, Eun-Jun Yoon, and Kee-Young Yoo, "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications," in **IEEE Access**, Vol. 5, pp. 3028-3043, 2017. **[This article is one of the top 50 most frequently downloaded documents for Popular Articles (May-June 2017)]**

Threat model

- We follow the widely-accepted Dolev-Yao threat (DY) model [1].
- Under the DY model, communication between two entities is performed over a public channel.
- An adversary can then have an opportunity to eavesdrop, modify or delete the content of the messages being transmitted.
- An adversary can physically capture one or more sensing devices in IoT, and can extract all the sensitive information stored in the captured devices using the power analysis attacks [2], [3].

[1] D. Dolev and A. Yao, "On the security of public key protocols," ***IEEE Transactions on Information Theory***, vol. 29, no. 2, pp. 198–208, 1983.
[2] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," ***IEEE Transactions on Computers***, vol. 51, no. 5, pp. 541–552, 2002.
[3] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in 19th Annual IACR Crypto Conference (Advances in Cryptology) - ***CRYPTO'99***, LNCS, vol. 1666, Santa Barbara, California, USA, 1999, pp. 388–397.

Contributions in this work

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

- An authentication model for IoT is presented and the security challenges involved and its requirements are discussed.
- A secure signature-based authentication and key agreement scheme has been proposed to address these issues.
- A formal security analysis using the widely-used Burrows-Abadi-Needham logic (BAN logic) and an informal security analysis have been presented to prove that the scheme is secure.
- Simulation using the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool for the formal verification of the scheme's security has also been provided.
- Using NS2 simulator, the scheme's impact on network performance parameters has been measured for practical demonstration of the scheme.
- Finally, it has been shown that the scheme is also efficient in terms of communication and computation costs.

Notations

Symbol	Description
GWN	Gateway node
SD_j	j^{th} sensing device
ID_j	SD_j's identity
U_i	i^{th} user
SC_i	U_i's smart card
ID_i	U_i's identity
PW_i	U_i's password
BIO_i	U_i's personal biometrics template
σ_i	Biometric secret key
τ_i	Biometric public reproduction parameter
t	Error tolerance threshold used by fuzzy extractor
$Gen(\cdot)$	Probabilistic generation procedure used by fuzzy extractor
$Rep(\cdot)$	Deterministic reproduction procedure used by fuzzy extractor
$h(\cdot)$	Collision-resistant one-way cryptographic hash function

Notations (Continued...)

Symbol	Description
p	A large prime number
Z_p	$Z_p = \{0, 1, \cdots, p-1\}$, a prime finite field
E_p	An elliptic curve over prime field Z_p
$P = ((P)_x, (P)_y)$	An elliptic curve point in elliptic curve E_p, $(P)_x$ and $(P)_y$ are x and y coordinates of P, respectively
$k.P$	Elliptic curve point multiplication; $k \in Z_p^*$ being a scalar and $P \in E_p$
d	private key of involved entities
Q	$Q = d.P$, public key of involved entities
T_i, T_s	Current system timestamps
ΔT	Maximum transmission delay
sk_{ij}	Session key between U_i and SD_j
$\oplus, \|\|$	Bitwise XOR and concatenation operations, respectively

Elliptic Curve Cryptography (ECC)

Elliptic curves over modulo a prime $GF(p)$

Let $p > 3$ be a prime. The elliptic curve $y^2 = x^3 + ax + b$ over Z_p is the set $E_p(a, b)$ of solutions $(x, y) \in E_p(a, b)$ to the congruence

$$y^2 \equiv x^3 + ax + b \pmod{p},$$

where $a, b \in Z_p$ are constants such that $4a^3 + 27b^2 \neq 0 \pmod{p}$, together with a special point $\mathcal{O}$ called the point at infinity (or zero point).

Properties of Elliptic Curves

- An elliptic curve $E_p(a, b)$ over Z_p (p prime, $p > 3$) will have roughly p points on it.
- More precisely, a well-known theorem due to Hasse asserts that the number of points on $E_p(a, b)$, which is denoted by $\#E$, satisfies the following inequality:

$$p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}.$$

- In addition, $E_p(a, b)$ forms an abelian or commutative group under addition modulo p operation.

Elliptic Curve Cryptography (ECC)

- **Point addition on elliptic curve over finite field** $GF(p)$
  If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be two points on elliptic curve $y^2 = x^3 + ax + b \pmod p$, $R = (x_R, y_R) = P + Q$ is computed as follows:

$$x_R = (\lambda^2 - x_P - x_Q) \pmod p,$$
$$y_R = (\lambda(x_P - x_R) - y_P) \pmod p,$$
$$\text{where } \lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} \pmod p, \text{ if } P \neq -Q \\ \frac{3{x_P}^2 + a}{2y_P} \pmod p, \text{ if } P = Q. \end{cases}$$

- **Scalar/point multiplication on elliptic curve over finite field** $GF(p)$
  If $P = (x_P, y_P)$ be a point on elliptic curve $y^2 = x^3 + ax + b \pmod p$, then $5P$ is computed as $5P = P + P + P + P + P$.

Elliptic Curve Cryptography (ECC)

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Definition (Elliptic Curve Discrete Logarithm Problem (ECDLP))

Let $E_p(a, b)$ be an elliptic curve modulo a prime p. Given two points $P \in E_p(a, b)$ and $Q = kP \in E_p(a, b)$, for some positive integer k, where $Q = kP$ represent the point P on elliptic curve $E_p(a, b)$ be added to itself k times. Then the elliptic curve discrete logarithm problem (ECDLP) is to determine k given P and Q.

Definition (Elliptic Curve Decisional Diffie-Hellman Problem (ECDDHP))

Let $E_p(a, b)$ be an elliptic curve and $G \in E_p(a, b)$ be a base point. The elliptic curve decisional Diffie-Hellman problem (ECDDHP) is defined as follows. Given a quadruple $(G, u.G, v.G, w.G)$, decides whether $w = u.v \pmod{p}$.

Biometrics and Fuzzy Extractor

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Definition

The fuzzy extractor is a tuple $(\mathcal{M}, l, t)$, which is composed of the following two algorithms, called *Gen* and *Rep*:

- **Gen:** It is a probabilistic algorithm, which takes a biometric information $B_i \in \mathcal{M}$ as input, and then outputs a secret key $\sigma_i \in \{0,1\}^l$ and a public reproduction parameter τ_i, where $Gen(B_i) = \{\sigma_i, \tau_i\}$.
- **Rep:** This is a deterministic algorithm, which takes a noisy biometric information $B_i' \in \mathcal{M}$ and a public parameter τ_i and t related to B_i, and then it reproduces (recovers) the biometric key data σ_i. In other words, we have $Rep(B_i', \tau_i) = \sigma_i$ provided that the condition: Hamming distance $d(B_i, B_i') \leq et$ is met.

One of the estimations on error tolerance threshold values provided by Cheon *et al.* is as follows: If the Hamming distance between the original biometric template B_i and current biometric template B_i' is h_T and the number of bits in input biometric is n_b, we then have $et = \frac{h_T}{n_b}$.

Biometrics and Fuzzy Extractor

- The probability to guess the biometric key data $\sigma \in \{0,1\}^l$ by an attacker is approximately $\frac{1}{2^l}$, where $l = m - 2\log(\frac{1}{\epsilon}) + O(1)$, where ϵ is the statistical distance between two given probability distributions, and m is the min-entropy given as follows. the min-entropy $H_\infty(A)$ of a random variable A is $-log(max_a Pr[A = a])$.

Vanga Odelu, Ashok Kumar Das, and Adrijit Goswami. "A Secure Biometrics-Based Multi-Server Authentication Protocol using Smart Cards," in **IEEE Transactions on Information Forensics and Security**, Vol. 10, No. 9, pp. 1953 - 1966, 2015, DOI: 10.1109/TIFS.2015.2439964. **[This article is one of the top 50 most frequently downloaded documents for Popular Articles (June - November 2015)]**

System Setup Phase

- *GWN* chooses a non-singular elliptic curve E_p over $GF(p)$ and a base point P of order n as large as the prime p.
- *GWN* also picks its private key d_{GWN} and computes the corresponding public key $Q_{GWN} = d_{GWN}.P$.
- *GWN* then chooses a collision-resistant one-way cryptographic hash function $h(\cdot)$, fuzzy extractor functions $Gen(\cdot)$ and $Rep(\cdot)$.
- The system parameters $\{E_p(a, b), p, P, h(\cdot), Q_{GWN}, Gen(\cdot), Rep(\cdot), t\}$ are made public, whereas d_{GWN} is kept secret by *GWN*.

Sensing Device Registration Phase

All the sensing devices in IoT are registered offline by the *GWN* as follows.

- For each device SD_j, the *GWN* chooses a unique identity ID_j and a unique private key d_j, and calculates the corresponding public key $Q_j = d_j.P$. It further computes $RID_j = h(ID_j \| d_j)$.
- The *GWN* pre-loads $\{ID_j, d_j, RID_j\}$ in the memory of SD_j. Furthermore, the *GWN* stores $\{ID_j, RID_j, Q_j\}$ in its database, and then makes Q_j as public.

User Registration Phase

User (U_i)	Gateway node (GWN)
Select identity ID_i, private key d_i. Compute public key $Q_i = d_i.P$ $RID_i = h(d_i \| ID_i)$. $\langle RID_i \rangle \xrightarrow{}$ (Secure channel)	Compute $R_i = h(RID_i \| d_{GWN})$. $\xleftarrow{\langle \text{Smart Card}\{R_i\} \rangle}$ (Secure channel)
Select password PW_i. Imprint personal biometric Bio_i. Compute $Gen(Bio_i) = (\sigma_i, \tau_i)$, $RPW_i = h(PW_i \| d_i \| ID_i \| \sigma_i)$, $R_i^* = R_i \oplus h(ID_i \| PW_i \| \sigma_i)$, $d_i^* = d_i \oplus h(ID_i \| \sigma_i)$. Insert $\{d_i^*, RPW_i, \tau_i, t, h(\cdot)$, $Gen(\cdot)$ and $Rep(\cdot)\}$ into smart card. Replace R_i with R_i^* in smart card.	