

MOŽNOSTI VYUŽITIA IOT TECHNOLOGIÍ PRI OCHRANE OSÔB A MAJETKU

Radoslav KUFFA, Filip LENKO, Andrej VELAS
Fakulta bezpečnostného inžinierstva, Žilinská univerzita v Žiline
Univerzitná 8215/1, 01026 Žilina, Slovensko
filip.lenko@fbi.uniza.sk

Abstrakt: *Internet vecí (IoT) je v súčasnej dobe veľmi vyžadovaný a začína sa vo veľkej miere implementovať do nových alebo už existujúcich bezpečnostných systémov na ochranu osôb a majetku. Pomocou IoT technológií môžu inteligentné zariadenia medzi sebou efektívne obojstranne komunikovať a pri zapojení viacerých medzi sebou vzniká vysoko inteligentný systém. V oblasti bezpečnosti je už v tejto dobe viacero inteligentných zariadení ako napr. kamery, rôzne čidlá. Systémy IoT majú za úlohu všetky tieto inteligentné zariadenia prepojiť, vyhodnocovať a riadiť. Príspevok sa zaoberá základnou koncepciou IoT, analýzou súčasného stavu a možnosťami využitia IoT v rôznych bezpečnostných oblastiach.*

Kľúčové slova: *internet vecí, bezpečnosť*

Abstract: *The Internet of Things (IoT) is currently in high demand and is beginning to be widely implemented in new or existing security systems to protect people and property. With the help of IoT technologies, intelligent devices can communicate effectively when they are connected to each other, a highly intelligent system is created. There are already several intelligent devices such as cameras, various sensors in the field of security. The role of IoT systems is connection, evaluate and control all these intelligent devices. The topic deals with the basic concept of IoT, analysis of the current state and the possibilities of using IoT in various security areas.*

Key words: *Internet of things, security*

Úvod

Internet vecí (IoT) preniká do nášho každodenného života. Postupom času sa pripája čoraz viac zariadení do internetu. Tieto zariadenia môžu pomocou internetovej infraštruktúry jednoducho komunikovať a takto vzniknuté systémy sa stávajú vysoko sofistikované. V princípe každé jedno zariadenie, ktoré vlastníme, alebo budeme vlastniť, sa dá pripojiť do internetu. Pomocou miniaturizácie a vznikom nových technologických a programovacích postupov je jednoduchšie vyvíjať malé, inteligentné a lacné zariadenia, ktoré dokážu nie len snímať a odosielať surové dáta, ale ich vedú podľa účelu spracovať a pripraviť pre ďalšie využitie. IoT z takýchto zariadení vytvára plnohodnotných používateľov internetu [2].

1 História IoT

Okamih, kedy sa dá začať hovoriť o IoT, je podľa skupiny Cisco Internet Business Solutions Group (IBSG), keď počet pripojených zariadení do internetu bude väčší ako počet obyvateľov planéty. V roku 2003 bolo na zemi približne 6,3 miliárd ľudí a zariadení pripojených do internetu bolo 500 miliónov. Podľa definície Cisco IBSG sa v tomto roku ešte nedalo hovoriť o IoT.

Obrovský rozmach chytrých telefónov, tabletov a počítačov prinieslo aj obrovské zvýšenie počtu pripojených zariadení. Tento rozmach nastal medzi rokmi 2008 až 2009. Podľa Cisco IBSG v týchto rokoch nastal zrod IoT. V roku 2010 bolo počet pripojených zariadení k internetu 12,5 miliárd, pričom ľudská populácia sa zvýšila na 6,8 miliárd [3]. V súčasnej dobe sme svedkami prudkého nárastu IoT riešení. Predpokladá sa, že do konca roku 2020 prekročí počet pripojených zariadení 20 miliárd [1].

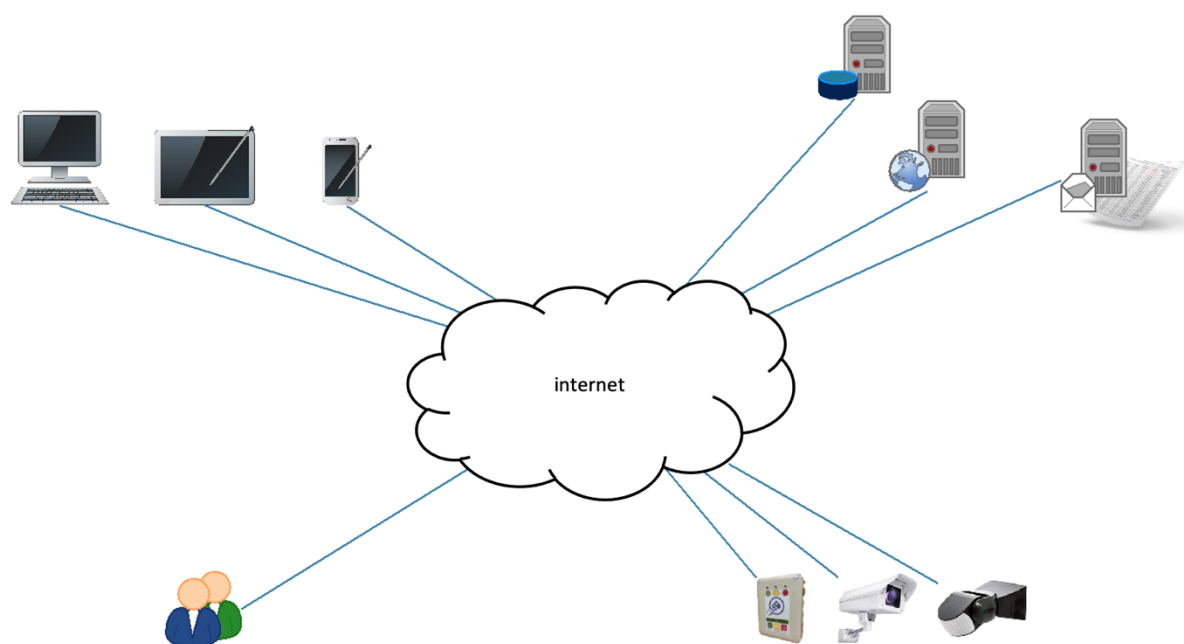
Rok	2003	2010	2020
Počet pripojených zariadení (miliárd)	0,5	12,5	20,0
Svetová populácia (miliárd)	6,3	6,8	7,8
Počet pripojení na jedného človeka	0,08	1,84	2,56



Obr. 1: Časové znázornenie zvyšovania pripojených zariadení v porovnaní ku svetovej populácii [2, 3, 4]

2 Základná koncepcia IoT

IoT je v podstate zapojenie rôznych zariadení do internetu, kde môžu spolu jednoducho a efektívne komunikovať. Tieto zariadenia sú jednoduché čidlá vytvorené pre jeden účel, zložitejšie zariadenia, až po veľmi sofistikované informačné systémy. Tieto medzi sebou komunikujú prostredníctvom internetovej siete. Medzi takéto pripojené zariadenia sa radia rôzne servery, vstupno/výstupné zariadenia ako sú mobily, tablety a počítače [3]. Keďže všetky technológie majú slúžiť ľuďom, je dôležité, aby bol človek do systému tiež pripojený a mohol ho v čase meniť, nastavovať a rozširovať [4].



Obr. 2: Typy pripojených zariadení

Hlavné stavebné bloky IoT

Zjednodušene môžeme povedať, že implementácia Internetu vecí zahŕňa štyri hlavné stavebné bloky (angl.: Blocks).

IoT stavebné bloky	IoT zariadenia	Funkcie
Veci (Things)	Senzory, akčné členy	Umožňujú komunikovať a zhromažďovať informácie z definovaných objektov bez interakcie človeka.
Brány (Gateways)	-	Pôsobí ako prechodný blok a umožňuje silné prepojenie medzi Vecami a Cloudovou infraštruktúrou. Poskytuje tiež bezpečnostné a správckové zabezpečenie počas toku údajov.
Sieťová infraštruktúra (Network Infrastructure)	Smerovač (Router), Prepínač (Switch), Brána Gateway), Opakovač (Repeater)	Umožňuje kontrolu toku údajov z Vecí do Cloudovej infraštruktúry. Zabezpečuje tiež bezpečnosť počas toku informácií.
Cloudová infraštruktúra (angl.: Cloud Infrastructure)	Virtualizované servery (Virtualized Servers), Dátové úložné jednotky (Data Storage Units)	Umožňuje analytické, logické a pokročilé výpočtové schopnosti.

Tab.1 Hlavné stavebné bloky IoT a ich popis [5]

Komponenty IoT

Pre ľahšie pochopenie implementácie Internetu Vecí a toku procesov uvedené štyri stavebné bloky môžeme zoskupiť do troch oblastí komponentov:

IoT komponenty	Funkcie
Veci so sieťovými senzormi a akčnými členmi (TNSA).	Zhromažďuje informácie z predmetov alebo vecí, ktoré boli definované podľa konkrétnej oblasti použitia.
Nespracované informácie a ukladané údaje (RI-PD-S) .	Uchováva zhromaždené informácie v rôznych formátoch: dáta, text, videá, obrázky, modely atď.
Analytické a výpočtové prostriedky (ACE).	Pomáha pri interakciách človek-stroj a umožňuje spätnú väzbu podľa používateľských požiadaviek.

Tab.2 Komponenty IoT a ich funkcie [5]

Interakcia komponentov IoT

Interakcia medzi komponentmi IoT začína od prvého komponentu TNSA. Senzory snímajú informácie, podľa požiadaviek používateľa. Zaznamenaná informácia sa potom uloží do druhého komponentu RI-PD-S, čo umožňuje interakciu medzi TNSA a RI-PD-S. Interakcia je umožnená odoslaním stavov správy a informácie sú uložené v rôznych formátoch, ako napr. údaje, text, videá a obrázky atď. Tretím komponentom IoT sú ACE, v ktorých sú uložené informácie logicky analyzované s použitím rôznych modelov. Táto logická analýza sa vykonáva pomocou viacerých opakovaných postupov, až kým sa nedosiahnu najlepšie výsledky podľa požiadaviek používateľa. V tomto treťom komponente je možné interaktívne učenie človek - stroj spolu s cloudovou a serverovou analýzou [6].

Oblasti konkrétneho využitia IoT

Hlavným prínosom IoT je vytvorenie kvalitnejších služieb pri využití už existujúcej infraštruktúry a existujúcich zariadení spolu s možnosťou vytvorenia zmeny alebo prípadného pridania nového prvku. Celková výhoda IoT sa odráža aj v znížení ceny takejto zmeny. Preto sa vyvíjajú stále nové aplikácie, ktoré môžu byť orientované napríklad na:

- inteligentné mestá,
- inteligentné domácnosti,
- inteligentné zdravotníctvo,
- inteligentné siete,
- inteligentné poľnohospodárstvo,

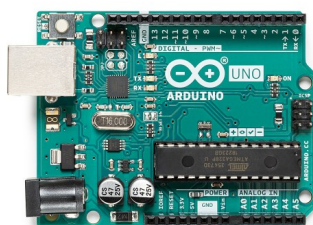
- inteligentná doprava [7].

Koncepcia IoT vykonáva výmenu dát nie len medzi prvkami konkrétnej oblasti, ale umožňuje komunikáciu aj medzi rôznymi nesúvisiacimi systémami. To znamená, že každá oblasť nie je uzavretý systém, ale môžu medzi sebou navzájom komunikovať. Nie je tu žiadne obmedzenie infraštruktúry a platformy. IoT povoľuje podporu rýchleho vývoja cez viaceré regióny, cez rôzne aplikácie a komunikáciu medzi službami systémov viacerých oblastí [8].

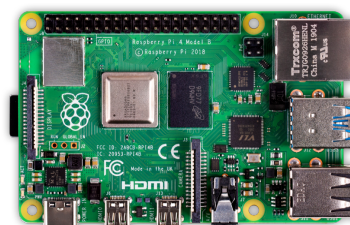
3 Súčasné možnosti IoT

Rozširovaniu aplikácií IoT systémov prispel veľký rozmach rôznych inteligentných zariadení s operačnými systémami jednoduchými na programovanie. Viaceré spoločnosti sa snažia vyvíjať svoje zariadenia tak, aby mohli ľudia, v podstate aj v domácom prostredí, upravovať a vytvárať rôzne riešenia. Ako najznámejšie operačné systémy sa pre tento účel využívajú Android, iOS, Windows, Linux. Viacerí výrobcovia zariadení sa snažia vytvárať a poskytovať svoje programovacie knižnice (SDK – Software development kit), ktoré obsahujú nástroje na vývoj aplikácií pre jednotlivé softvérové platformy.

Na rozmach internetu a IoT reagujú aj spoločnosti, ktoré vyrábajú rôzne mikropočítače alebo vývojové dosky. Medzi najznámejšie patria Raspberry Pi a Arduino.



Arduino



Raspberry Pi

Obr. 3: Mikropočítač Raspberry Pi a vývojová doska Arduino

Zariadenia tohoto typu majú veľké množstvo rozšírení. Každé takéto zariadenie dokáže vykonávať zber dát z reálneho sveta, následne ich spracovať a poskytnúť prostredníctvom internetu ďalším zariadeniam alebo systémom.

Na druhej strane sa dajú takéto dosky využiť ako medzistupeň, ktorý spracuje a pripojí akékoľvek zariadenie k internetu a nakoniec mu poskytne výhody IoT zariadení. Napríklad môžeme uviesť prepojenie elektronickej požiarnej signalizácie (EPS) cez výstupné relé.

4 Využitie IoT pri bezpečnostnom incidente – vstup do kritickej oblasti

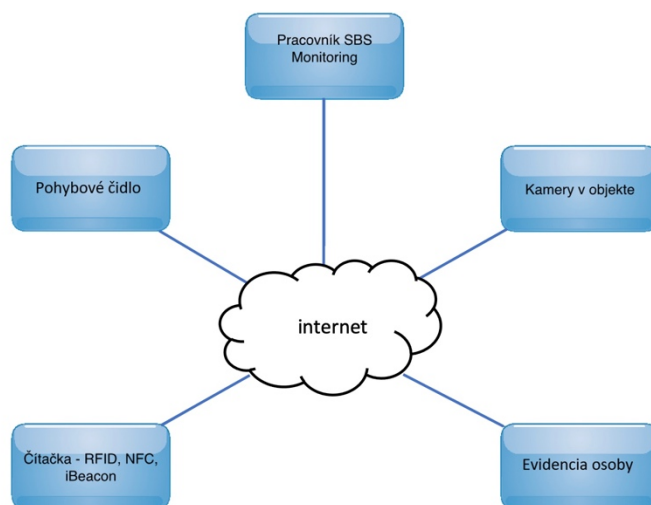
Z uvedeného vyplýva, že pre zostavenie efektívneho bezpečnostného systému nemusíme spájať len zariadenia zamerané na bezpečnosť. Z každého zariadenia pripojeného do internetu v rámci IoT systému vieme zužitkovať dáta pre viaceré oblasti. Z toho dôvodu pre zostavenie IoT bezpečnostného systému môžeme využívať zariadenia napr. z dopravy alebo výroby. Kombinácia jednotlivých prvkov je neobmedzená a dôležité je, že je možné konfigurácie v čase meniť.

4.1 Bezpečnostný incident v objekte

Predpokladáme situáciu, keď známa osoba vstúpi do objektu (zamestnanec, návšteva). Osoba sa pohybuje v objekte a vykonáva činnosti v súlade s jeho oprávneniami. Pracovník SBS pomocou výstupov z IoT systému priebežne monitoruje jeho pohyb.

V určitom čase nastáva situácia, keď osoba vstupuje do oblasti, kde je nutné vyhodnotiť, či má na vstup do tejto oblasti oprávnenie.

4.2 Příklad prepojenia a funkcionality zariadení



Obr 4: Pripojené typy zariadení využitých pre bezpečnosť

1. Evidencia vstup do objektu - Identifikovanie osoby v systéme:
 - zaznamenanie údajov o osobe,
 - priradenie dočasného systémového identifikátora osoby.
2. Čítačka – identifikovanie osoby v určitej oblasti:
 - RFID, NFC – osoba priloží identifikačnú kartu ku čítaciemu zariadeniu,
 - iBeacon – osoba má pri sebe Bluetooth Low Energy (BLE) čip a snímacie zariadenie vyhodnotí prítomnosť osoby v oblasti.
3. Pohybové čidlo – vyhodnotenie narušenia kritických oblastí na základe pohybu
4. Kamery v objekte – využitie inteligentných funkcionalít kamery
 - vyhodnotenie pohybu v snímanej oblasti,
 - vyhodnotenie vstupu do vyznačenej oblasti,
 - online prenos obrazu,
 - nahrávanie obrazu.

4.3 Zistenie a vyhodnotenie incidentu

Priebežné získavanie údajov

Pri vstupnej evidencii sa priradí osobe jednoznačný identifikátor. Tento sa priradí ku vstupnej karte s RFID, NFC alebo iBeacon čipom.

Počas celého pohybu osoby v objekte je tento čip monitorovaný rôznymi zariadeniami. Dáta o polohe sú neustále zaznamenávané a odosielané. Čítacie zariadenie môže byť napojené na ďalšie technológie ako otváranie dverí, zapnutie osvetlenia. Inteligentné čítacie zariadenie vykonáva činnosti buď samostatne pomocou vlastného vyhodnotenia, alebo sa dopytuje na riadiacu jednotku. Riadiaca jednotka je tiež súčasťou IoT.

Ďalším zariadením, ktoré sa dá využiť na trasovanie je kamera. Rozpoznávanie obrazu kamerou môže byť v určitých prípadoch so zvýšenou chybovosťou, ale kombináciou viacerých zariadení vieme chybovosť podstatne znížiť. Pravdepodobnosť zaznamenania vstupu osoby do určitej oblasti sa podstatne zvýši, keď takýto vstup vyhodnotia dve a viac zariadení súčasne. Popri tom použitím takejto kombinácie zvyšujeme aj spoľahlivosť, keďže pri výpadku jedného zariadenia máme dáta z iného. (Pri strate alebo zničení prístupovej karty dostávame dáta z kamier.)

4.4 Vznik incidentu

Signál narušení kritickej oblasti dostávame z pohybového čidla. Systém na základe viacerých informácií, ktoré priebežne zbiera, vyhodnotí pravdepodobnosť narušenia. Na základe dát z trasovania osoby vyhodnotí, ktorá osoba sa v oblasti nachádza. Ak osoba nemá oprávnenie vstupovať do oblasti, systém vykoná dopredu nastavené úkony:

- blokovanie dverí oblasti,
- spustenie sirény,
- notifikácia monitorovaciemu centru,
- zobrazenie konkrétnych kamier obsluhu (len kamery z kritickej oblasti).

Celý IoT systém na základe viacerých dát vyhodnotí a ponúkne obsluhu najlepšie riešenie. Pracovník strážnej služby má systémom ponúknuté podrobné informácie o pohybe osoby v objekte a o vzniknutom incidente.

Záver

Oblasť IoT technológií je v súčasnej dobe veľmi dynamická. Každým dňom sa pripájajú do internetu ďalšie a ďalšie zariadenia. Dôležité je si uvedomiť, že IoT technológie nám poskytujú komunikáciu medzi zariadeniami bez zložitej infraštruktúry. Vedia medzi sebou komunikovať naprieč regiónmi aj naprieč platformami. Toto nám poskytuje veľké možnosti v skladaní jednotlivých koncových zariadení do veľkých celkov a tým vytvárať sofistikované systémy.

Prax v bezpečnostných oblastiach nám ukazuje vzájomnú prepojenosť s inými oblasťami. Informácie získané zariadeniami určenými napr. pre riadenie dopravy sú cenným zdrojom informácií pri zisťovaní bezpečnostných incidentov. Preto oblasť IoT technológií poskytuje bezpečnostnej oblasti prepojenie a využitie dát, ktoré sa dajú využiť aj na iný účel.

Keďže sú IoT technológie zvyčajne pripojené k internetu, môžu byť napadnuteľné, čo môže mať vplyv aj na ich spoľahlivosť. Z hľadiska bezpečnosti tak nie je vhodné ich využívať v bezpečnostných aplikáciách, ktoré vyžadujú vysoký stupeň zabezpečenia. Ako sme uviedli v našom príklade, pokiaľ sa jedná o uzavretý systém a IoT technológie slúžia ako doplnok k existujúcemu poplachovému systému, ich spoľahlivosť a bezpečnosť bude na vysokej úrovni.

Literatúra

- [1] ŠPRLÁK, A. 2020. Inovácia vybraného bezpečnostného prvku. [Diplomová práca]
- [2] CRAIG L., FUMAGALLI A. 2019. *Internet of Things Security - Multilayered Method For End to End Data Communications Over Cellular Networks*. 2019 IEEE 5th World Forum on Internet of Things (WF-IoT)
- [3] EVANS D. 2011. *The Internet of Things - How the Next Evolution of the Internet Is Changing Everything*. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
- [4] DIWAN P. 2018. Pervasiveness of IoT in Our Daily Life. <https://medium.com/@pdiwan/pervasiveness-of-iot-in-our-daily-life-68019de028ee>
- [5] Gebremichael, T., Ledwaba, LPI., Eldefrawy, MH., Hancke, GP., Pereira, N., Gidlund, M., Akerberg, J. 2020. *Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges*. IEEE ACCESS, ISSN: 2169-3536.
- [6] Bicaku, A., Tauber, M., Delsing, J. 2020. *Security standard compliance and continuous verification for Industrial Internet of Things*. INTERNATIONAL JOURNAL OF DISTRIBUTED SENSOR NETWORKS, ISSN: 1550-1477.
- [7] DONGXIAO YU, XIUZHEN CHENG, FALKO DRESSLER, KOWALSKI D., WEIFENG. 2020. *Guest Editorial: Special Issue on High-Confidence City IoT for Collaborative Smart City Services*. IEEE Internet of things journal, VOL. 7, NO. 9, SEPTEMBER 2020
- [8] Ma, Y., Wu, C., Ping, K., Chen, H., Jiang, CB., 2018. *Internet of Things applications in public safety management: a survey*. LIBRARY HI TECH, ISSN: 0737-8831.