ARTICLE:1

**IoT Based Child Safety Locator From Water and Fire**

Md Rony, Minhajul Islam, Sanjida Khanam, Sagar Gosh

Daffodil International University, 2021

This project is an IoT based development project titled “IoT Based Child Safety Locator from Water and Fire”. For the past few years, the child date rate has been a major concern, particularly in our country. This IoT based development project is designed & built for general people who don’t need any depth knowledge of using digital technology. This project is mainly focused to reduce the child death rate. Also, this can ensure the awareness of parents for the children. In this system we used node MCU, GPS module and many other components but

A Smart Protection Device. Savan Gondaliya, Rahil Khalak, Priyanka Mistry, Adolf Sibanda, Keyaben S Patel

Human security is need of the hour in present times. Across the globe, there are many cases of unknown attacks, harassment and molestation. Safety of an individual matters whether it is at home, outdoor or their work place. We propose an idea which changes the way everyone thinks about once individual’s safety, a day when media broadcasts more of achievements rather than harassment. Since we (humans) can't respond rapidly in critical situations, the need for a device which effectively rescues the victim is the venture of our idea in this project. We are proposing Arduino Nano and Alarm Grenade (sonic weapon) based portable device which can be effective in both in network and network outage scenarios. This device can be classified in 3 parts based on functionality.

ARTICLE:2

**Smart Child Monitoring Device**

Pushpendra Kumar Pateriya, Parminder Singh, RU Jitesh, Shivam Gumber

Think India Journal 22 (3), 8079-8089, 2019

In this era most of the families are nuclear family, and husband wife both work to cope up with the needs of family. So it becomes tough for the parents to monitor their baby or infant all the time. In such a situation working parents hire a babysitter and pay a handsome amount of salary to her. Parents want to monitor babysitters also because they do not trust them completely. Few of the baby monitoring tasks (ie ambience monitoring, skin temperature monitoring, strangers’ recognition, abnormalities monitoring, and instant alert generation etc.) can be done using IoT enabled technological solutions. In this paper we have proposed a smart child monitoring system which can monitor a baby effectively, can generate instant alerts and save baby health related data on cloud for further analysis.

ARTICLE:3

**Review Paper on Safety Devices for Women**

G Ranjithkumar, V Voorwashi, T Anuradha

Innovations in Signal Processing and Embedded Systems, 359-371, 202In today's culture, women face several security issues. They feel insecure in such situations and require assistance to defend themselves. Even though numerous technological advancements have been made for women, kidnappings, eve teasing, and harassment continue to occur in our society. To protect the safety of women in insecure circumstances, an automatic detection system must be established that will deliver an alarm message with the police department's address. This may be accomplished by monitoring different elements such as, Node MCU, flex sensors, and pulse sensors, all of which can be detected with the use of sensors, and sending an alarm message. The present method for detecting locations, delivering messages, and gathering

ARTICLE:4

**Security engineering: a guide to building dependable distributed systems**

Ross8 Anderson

John Wiley & Sons, 2020

Now that there's software in everything, how can you make anything secure? Understand how to engineer dependable systems with this newly updated classic In Security Engineering: A Guide to Building Dependable Distributed Systems, Third Edition Cambridge University professor Ross Anderson updates his classic textbook and teaches readers how to design, implement, and test systems to withstand both error and attack. This book became a best-seller in 2001 and helped establish the discipline of security engineering. By the second edition in 2008, underground dark markets had let the bad guys specialize and scale up; attacks were increasingly on users rather than on technology. The book repeated its success by showing how security engineers can focus on usability. Now the third edition brings it up to date for 2020. As people now go online from phones more than laptops, most servers are in the cloud, online advertising drives the Internet and social networks have taken over much human interaction, many patterns of crime and abuse are the same, but the methods have evolved. Ross Anderson explores what security engineering means in 2020, including: How the basic elements of cryptography, protocols, and access control translate to the new world of phones, cloud services, social media and the Internet of Things Who the attackers are–from nation states and business competitors through criminal gangs to stalkers and playground bullies What they do–from phishing and carding through SIM swapping and software exploits to DDoS and fake news Security psychology, from privacy through ease-of-use to deception The economics of security and dependability–why companies build vulnerable systems and governments look the other way How dozens of industries went online–well or badly How to manage security and safety engineering in a world of agile development–from reliability engineering to DevSecOps The third edition of Security Engineering ends with a grand challenge: sustainable security. As we build ever more software and connectivity into safety-critical durable goods like cars and medical devices, how do we design systems we can maintain and defend for decades? Or will everything in the world need monthly software upgrades, and become unsafe once they

ARTICLE:5

**Globalized (in) security: the field and the ban-opticon**

Didier Bigo
Terror, insecurity and liberty, 20-58, 2008
The discourses that the United States and its closest allies2 have put forth asserting the necessity to globalize security have taken on an unprecedented intensity and reach. They justify themselves by propagating the idea of a global '(in)security', attributed to the development of threats of mass destruction, thought to derive from terrorist or other criminal organizations and the governments that support them. This globalization is supposed to make national borders effectively obsolete, and to oblige other actors in the international arena to collaborate. At the same time, it makes obsolete the conventional distinction between the universe of war, defence, international order and strategy, and another universe of crime, internal security, public order and police investigations. Exacerbating this tendency yet further is the fact that, since 11 September 2001, there has been ongoing frenzied speculation throughout the Western political world and among its security 'experts' on how the relations between defence and internal security should be aligned in the new context of global (in)security.

ARTICLE:6
**IoT-Based Delineation and Evolution of Kid's Safety Portable Devices**
H Hemasundari, B Swapna
Handbook of Research on Innovations and Applications of AI, IoT, and Cognitive Technologies, 148-157, 2021 Currently there are numerous portables in the retail which assist tracking the day-by-day actions of kids and furthermore help discover the kid utilizing Wi-Fi and Bluetooth directions available on the gadget. Bluetooth gives off an impression of being an untrustworthy mode of correspondence connecting the parent and kid. Along these lines, the pivotal motive of this chapter is to get an authorized corresponding medium that links the kid's portable and the parents. The genitor can send a book with explicit tags, for example,"location,""temperature,""UV,""SOS,""BUZZ," and so forth. The portable device will response with a book encompassing the continuous precise region of the kid, which after monitoring hand down headings to the youngster's region on Google Maps software will similarly provide the atmospheric temperature and UV ray emission file with a goal that genitors can pursue if temperature or UV emission isn't reasonable to the kid.

ARTICLE:6
**Network-level security and privacy control for smart-home IoT devices**
Vijay Sivaraman, Hassan Habibi Gharakheili, Arun Vishwanath, Roksana Boreli, Olivier Mehani
2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob), 163-167, 2015

The increasing uptake of smart home appliances, such as lights, smoke-alarms, power switches, baby monitors, and weighing scales, raises privacy and security concerns at unprecedented scale, allowing legitimate and illegitimate entities to snoop and intrude into the family's activities. In this paper we first illustrate these threats using real devices currently available in the market. We then argue that as more such devices emerge, the attack vectors increase, and ensuring privacy/security of the house becomes more challenging. We therefore advocate that device-level protections be augmented with network-level security solutions, that can monitor network activity to detect suspicious behavior. We further propose that software defined networking technology be used to dynamically block/quarantine devices, based on their network activity and on the context within the house such as time-of-day or occupancy-level. We believe our network-centric approach can augment device-centric security for the emerging smart-home.

OBJ

ARTICLE:7

Wearable Device for Child Safety using Arduino Uno and Tracking System

J Angurajsiva, V Elakkiya, A Kowsalya, S Ramya, S Divya

International Research Journal of Innovations in Engineering and Technology 4 (5), 105, 2020 This task depends on GSM based innovation to give wellbeing to kid, which would be controlled from anyplace else. The target of this task is to give a security to kid utilizing remote innovation. The fundamental target of this venture is screen the youngster utilizing RF remote correspondence. We can likewise observing a wellbeing level of kid utilizing Heart beat sensor. Area of youngster is found by GPS if there should be an occurrence of crisis. If there should be an occurrence of crisis the SMS sent by means of GSM to kid guardians and family members portable, GPS gives just the longitude and scope esteems yet by utilizing GSM modem to versatile we can without much of a stretch get the area name from where the message has been sent. The controller accepts the sensors as its info for example at the point when some risk has happened one have to changes in sensor esteem and the controller makes the GSM modem to warning to the pre-put away in server. Right now concerned individual will know the area and they will have the option to spare the competitor. With a wide scope of sequential interchanges interfaces, they are additionally very appropriate for correspondence doors, convention converters and installed delicate modems. Expansion to this reason framework sensors is additionally their at whatever point the youngster cross certain separation over his folks region and somebody hijacked a kid around then we get the area to safe them.

ARTICLE:8

**Network-level security and privacy control for smart-home IoT devices**

Vijay Sivaraman, Hassan Habibi Gharakheili, Arun Vishwanath, Roksana Boreli, Olivier Mehani

2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob), 163-167, 2015 The increasing uptake of smart home appliances,

such as lights, smoke-alarms, power switches, baby monitors, and weighing scales, raises privacy and security concerns at unprecedented scale, allowing legitimate and illegitimate entities to snoop and intrude into the family's activities. In this paper we first illustrate these threats using real devices currently available in the market. We then argue that as more such devices emerge, the attack vectors increase, and ensuring privacy/security of the house becomes more challenging. We therefore advocate that device-level protections be augmented with network-level security solutions, that can monitor network activity to detect suspicious behavior. We further propose that software defined networking technology be used to dynamically block/quarantine devices, based on their network activity and on the context within the house such as time-of-day or occupancy-level. We believe our network-centric approach can augment device-centric security for the emerging

ARTICLE:9

**Solution integration approach using iot in education system**

Suja P Mathews, R Raju Gondkar

International Journal of Computer Trends and Technology (IJCTT) 45 (1), 2017

While several institutions contributes significantly to technology, the leveraging this has been limited due to technological challenges and also cost implications. Internet of Things based cloud systems has a tremendous potential to enable educational institutions to leverage the advances in the cost effective cloud systems. This paper describes the various technologies that can be used for collecting data, managing them on the cloud and using analytics for maintaining the overall campus infrastructure. A high level architecture to connect these various technologies to the cloud is also proposed. This would enable a centralized system, which can address e-learning, student tracking and security, in-campus and indoor navigation, and also student management.

ARTICLE:10

**Implementation of Novel Application for Woman and Child Protection Using IOT Enabled Techniques.**

Khasim Shaik, Santoshi Bogaraju, Sagar Vadepu

International Journal of Advanced Research in Computer Science 8 (3), 2017

Today in present global computing world most of the scenarios which are all based upon digital technology and moreover every person is connected with each other in many number of ways, where in which most popular communication is all the times as an Internet. In current global scenario, the harassment of women and children are increased day-by day and the world is becoming more unsafe and helpless. The most common incidents that are raised upon women and children are chain snatchings, kidnapping, sexual harassments, eve teasing, etc., and the worst among all mentioned in previous is rape which is rising in many countries. The only thought of haunting every girl is when they move in odd hours or alone without worrying about their security. In such perilous situations there must be a mechanism to be implemented that they easily affordable and comfortable to handle those situations instantly. In this paper we proposed a device which is integrated with multiple devices, comprising of wearable" smart

band" which is connected to the smart phone through the BLE module. The smart phone that has the application which is programmed with all the required data which includes the behaviour of the human and reactions like anger, anxiety, nervousness and fear. When these situations are faced by the victim, the various sensors generates the emergency signals which are to be transmitted to the smart phone. Based on the transmission, the GPS tracks the location and GSM sends help request by sending messages to the nearest police station, relatives and the people in the near radius through Google map link to save the person. This type of system plays a crucial role to ensure safety of women and children in the fastest way.

ARTICLE:11

**Activity tracker wrist band for children monitoring using IOT**

T Bhanupriya, TV Sundarajan, S Raja

Int J Recent Innov Trends Comput Commun 6 (5), 2018

Today in introduce universe of advanced innovation and worldwide figuring each individual is associated with each other in number of ways. In current worldwide figuring world, the youngsters and ladies provocation, chain snatchings, hijacking, lewd activities, eve prodding, and so forth are expanded step by step, winding up more perilous and powerless. At the point when these risky circumstances happen there must be an inclining innovation to be agreeable to deal with. So we are proposing a framework that takes a shot at the debate of youngsters utilizing IOT. In this venture we proposed a gadget which is incorporated with different gadgets, containing wearable" Action Tracker Wrist Band" which is modified with all the required information which incorporates the conduct of the human responses like outrage, uneasiness, anxiety and dread. At the point when these circumstances are looked by the casualty, the different sensors produce the crisis signals which are to be transmitted to the advanced cell. The framework adequately screens the kids nearness inside the normal zone. At the point when the individual crosses the checking zone, at that point in light of IOT Monitoring framework, GSM sends help ask for by sending messages to the closest police headquarters, guardians and the general population in the close sweep.

ARTICLE:12

**IoT Based Smart Gadget for Child Safety and Tracking**

N Manjunatha, HM Jayashree, N Komal, K Nayana

This paper is mainly streamed towards child safety solutions by developing a gadget which can be tracked via its GPS locations and also a panic button on gadget is provided to alert the parent via GSM module calling for help. Parental android app is developed to manage and track the device anytime. Smart gadget device is always connected to parental phone which can receive and make phone calls and also receive SMS on gadget via GSM module, also a wireless technology is implemented on device which is useful to bound the device within a region of monitoring range, if device is moving out of monitoring range then an alert will be triggered on binding gadget, this helps you keep a virtual eye on child. Health monitoring system on gadget checking for parameters like heart beat/pulse rate and temperature is included which can be monitored on parental app. Gadget also monitors whether it is plugged on hand or not using contact switch and alert the parent as soon as it is unplugged.

ARTICLE:12

**Design of Wearable Device for Child Safety**

M Benisha, R Thandaiah Prabu, M Gowri, K Vishali, M Anisha, Ponmozhi Chezhiyan, C Jim Elliot 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 1076-1080, 2021 Now-a-days attacks on children are increasing at an unprecedented rate and the victims are in dangerous conditions, where they are not allowed to contact the family members. The key idea planned in this research work is an advanced technology that offers “Smart Child Safety” for the children. Therefore, the awareness of this method is to send an SMS fromchildren's wear tool to their parent or guardian. In the prevailing structure, there is no monitoring method for child, it should create many problems for them and the no protection mechanism to protect the child from the misbehavior. In addition, there is no aware device for the child's protection; it must be completed by hand only. Thus, the planned method will be highly effective when compared to the other existing techniques in helping the victims. Moreover, it doesn't need any manual operation. This paper recommends a newfangled technology for child protection by using GSM so that the children will not feel abandoned while facing such social problems. The problems overawed here using Arduino UNO, GSM, sensors, MEMS, temperature and panic button by using IOT. In such case, Heartbeat Sensor track the best rate for children and sends the emergency message by using the GSM to save contacts. Such method is actually supportive for children in today's world. Hence, this provides a security to the children and secures the feeling of parents

ARTICLE:13

**COVID-SMD: CHILD OLDSTER VICTIM ILL DUMB-SAFETY MONITORING DEVICE**

Mansi Kashyap, Shuchita Saxena, Kshitij Shinghal, Amit Saxena
International Journal of Advances in Engineering & Technology 13 (4), 123-130, 2020
Pablo Picasso quoted" Without great solitude, no serious work is possible". COVID-19 the deadly widespread epidemic taught this that in desolation one can come up with a great idea and some out of the box suggestion or design. This paper presents such project that is made in solitariness due to the pandemic. Here a prototype is described for the frontline warriors of novel Corona virus. Besides this it would also be very helpful for monitoring of health, activities and tracking our loved ones. The prototype is named as COVID-SMD and abbreviated as Child Oldster Victim Ill Dumb Safety Monitoring Device. It consists of five modules which would tell us about the temperature, surrounding light, fall, removal of the device and emergency situation. It would monitor the temperature of the wearer, will keep a track of location, alert about the fall of the person, detect if person is in dark and will also help your loved ones in their panic situation. It will send alert messages to the phone number saved in the source code. This device would be productive for both parents who want to monitor their kiddos, as well as for children to supervise their golden age geriatric parents. It would be essential for the person suffering from various diseases such as dementia (short term and long-term memory loss), autism (nervous breakdown), Alzheimer (loss of functioning of brain). At present time of Pandemic Safety and monitoring of children, elderly people, dumb people handicapped, patients where social distancing is very important

**Advanced Child Tracking Monitoring System**

G Praveen Kumar

This project is based on safety preventive solutions, provided in school's campus to avoid child abuse, child molestation, and child bullying, medical emergencies. We have come up with an innovative idea to prevent all this, it's a wearable devise which is continuously read by our sensors and find out if there is any emergency. It's a smart software is triggers soft alerts to the command center people stating that so and so kid is with xyz person in an isolated place. Rescue team check the scene and stops if anything is wrong is happening. Every person in the campus should wear the devise (teaching staff and non-teaching staff) visitors will be given the devise at the time of entry to the campus.

ARTICLE:14

**How can parents support children's internet safety?**

Andrea Duerager, Sonia Livingstone

EU Kids online, 2012

Given the Safer Internet Day 2012 theme of Connecting Generations, we ask whether, instead of imposing restrictions, parents can support their child's internet safety by sharing a positive experience of internet use with them. An analysis of parental mediation in the EU Kids Online survey of 25,142 9-16 year olds in 25 countries shows that restrictive mediation reduces online risks, but it also reduces their online opportunities and skills. The new analysis in this report shows that when parents actively mediate their child's internet use, this too is associated with lower risk and, most important, lower harm. However, parental active mediation of use is linked to more (not fewer) online activities and skills

ARTICLE:15

**Enhanced Child Activity Monitoring Tool**

P Karhik

Enhanced child activity monitoring tool by JAG & WYT solutions is a child safety product for schools, to track the child in real-time during school hours. Decreasing weight of labor and giving guardian's alleviation that their kid is sheltered. Our Software Cum Hardware display is intended to give the correct area of tyke inside the campus.it help the youngster to call for help or the delicate cautions if there's anything suspicious around the kid, say if the kid ought to be in class and is in some detached

place the product triggers the alert expressing that the kid is in disconnected place with XYZ individual protect group checks what is the scene and safe watches the place Every person who works in campus teaching and non-teaching staff, children, and any other person who comes inside the campus should wear the devise. It helps finding who is there in which place and analyze the need for help and prevent child abuse, medical emergency, child bullying etc., in order to give a safe educational environment. There may be lot of solutions today, but they are not effective since camera can only record the incident and cannot prevent them, GSM based can only alert the parents and does not help in prevention, RFID not applicable as it does not help in tracking the child, GPS/GPRS - Not effective as it has limitations in tracking the child within enclosures, Our product helps in proving this solutions and give a safer environment to

the students. ENHANCED CHILD ACTIVITY MONITORING TOOL 1NH16MCA72 Department of Master of Computer Applications, NHCE, Bangalore 2017-2018 2 Child safety is the most significant component encouraged to develop and advanced technology in order to give a safer place. Lot of incidents forced to innovation and brings in new ways of safeguarding to provide secure life for child in campus. Parents lost their trust on security in schools and are not comfortable until the child resumed back to home safely.

ARTICLE:16

**Implementation of Child Safety Alert System in Automobiles**

Eeda Srinavya, Maddula Bhaswitha, S Siva Vineeth, BK Priya

2021 2nd Global Conference for Advancement in Technology (GCAT), 1-6, 2021

Every year lot of children are passing away due to hyperthermia and coronary heart strokes. This is happening because the children are left inside the car unknowingly. Many incidents of such cases are increasing rapidly in the past few decades. These incidents are recognized as the automobile injuries and for this a research has been done to know more about the fat situations of the surroundings of such instances. By the research it is known that there are two elements which made the kids more liable to hyperthermia when compared to adults. A systematic rationalization about how this can be appeared that the children are left unknowingly by their parents in the vehicle can be identified with working memory, it builds up the pressure obstruction and impends to a particular interest. In pasttwo years, 16 children of these cases in Italy and 53 children of these cases in US of infant hyperthermia because of abandonment in vehicles were perceived. These discoveries propose that instructive bundles and writing for guardians concerning auto insurance should incorporate such data about these threats of the heart stress, in fact such actions are unknowingly happened and not intentionally done. In triumph over these issues a prototype has been proposed by means of the child safety alert system.

ARTICLE:17

**Arkangel and Parental Surveillance: What are a Parent's Obligations?**

Catherine Villanueva Gardner, Alexander Christian

Black Mirror and Philosophy: Dark Reflections, 151-159, 2019

“Archangel” explores the consequences of Marie's over-parenting of her daughter, Sara, through the use of a neural implant (the Archangel) that allows Marie to track (and block) Sara's experiences. In attempting to fulfill her duty to protect Sara, Marie ultimately fails morally as a parent. What is fascinating is that different schools of philosophical thought – contemporary liberal philosophy, ancient Greek Aristotelian ethics, contemporary feminist ethics of care, and contemporary Wittgensteinian ethics – all reach the same conclusion about Marie's moral failure, while teasing out different strands of this failure.

ARTICLE:18

**Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations**

Nataliia Neshenko, Elias Bou-Harb, Jorge Crichigno, Georges Kaddoum, Nasir Ghani

IEEE Communications Surveys & Tutorials 21 (3), 2702-2733, 2019

The security issue impacting the Internet-of-Things (IoT) paradigm has recently attracted significant attention from the research community. To this end, several surveys were put forward addressing various IoT-centric topics, including intrusion detection systems, threat modeling, and emerging technologies. In contrast, in this paper, we exclusively focus on the ever-evolving IoT vulnerabilities. In this context, we initially provide a comprehensive classification of state-of-the-art surveys, which address various dimensions of the IoT paradigm. This aims at facilitating IoT research endeavors by amalgamating, comparing, and contrasting dispersed research contributions. Subsequently, we provide a unique taxonomy, which sheds the light on IoT vulnerabilities, their attack vectors, impacts on numerous security objectives, attacks which exploit such vulnerabilities, corresponding remediation methodologies and currently offered operational cyber security capabilities to infer and monitor such weaknesses. This aims at providing the reader with a multidimensional research perspective related to IoT vulnerabilities, including their technical details and consequences, which is postulated to be leveraged for remediation objectives. Additionally, motivated by the lack of empirical (and malicious) data related to the IoT paradigm, this paper also presents a first look on Internet-scale IoT exploitations by drawing upon more than 1.2 GB of macroscopic, passive measurements' data. This aims at practically highlighting the severity of the IoT problem, while providing operational situational awareness capabilities, which undoubtedly would aid in the mitigation task, at large. Insightful findings, inferences and outcomes in addition to open challenges and research problems are also disclosed in this paper, which we hope would pave the way for future research endeavors addressing theoretical and empirical aspects related to the imperative topic of IoT security.

ARTICLE:19

**Design and Implementation of Security Device for Patient Health Monitoring Systems**

AK Sahu, NK Misra, D Kumar

IOP Conference Series: Materials Science and Engineering 1119 (1), 012003, 2021

In continuous upgrading world, humans believe in their self-worth. They have participation in every sector of life, but lives have become so vulnerable these days that the safety and security of their lives are one of the burning questions about this pandemic corona virus disease. Considering all incidents and violation of rules do not spread against humanity this idea of a smart wristband safety device aligned with GPS and GSM modules, with temperature and pulse sensors came into consideration. During dangerous situations user just needs to press the SOS button fitted on the wristband, or the sensors will sense an increase in temperature or pulse rate and then automatically the message of user location tracking via GPS will be sent to the registered numbers through GSM. The main objective is for the device to be light weight and place the SOS switch in an easy accessible region, with additional sensors leaving no worse case possible.

ARTICLE:20

**Anatomy of threats to the internet of things**

Imran Makhdoom, Mehran Abolhasan, Justin Lipman, Ren Ping Liu, Wei Ni

IEEE communications surveys & tutorials 21 (2), 1636-1675, 2018

The world is resorting to the Internet of Things (IoT) for ease of control and monitoring of smart

devices. The ubiquitous use of IoT ranges from industrial control systems (ICS) to e-Health, e-Commerce, smart cities, supply chain management, smart cars, cyber physical systems (CPS), and a lot more. Such reliance on IoT is resulting in a significant amount of data to be generated, collected, processed, and analyzed. The big data analytics is no doubt beneficial for business development. However, at the same time, numerous threats to the availability and privacy of the user data, message, and device integrity, the vulnerability of IoT devices to malware attacks and the risk of physical compromise of devices pose a significant danger to the sustenance of IoT. This paper thus endeavors to highlight most of the known threats at various layers of the IoT architecture with a focus on the anatomy of malware attacks. We present a detailed attack methodology adopted by some of the most successful malware attacks on IoT, including ICS and CPS. We also deduce an attack strategy of a distributed denial of service attack through IoT botnet followed by requisite security measures. In the end, we propose a composite guideline for the development of an IoT security framework based on industry best practices and also highlight lessons learned, pitfalls and some open research challenges.

ARTICLE:21

**Child safety monitoring system based on IoT**

N Senthamilarasi, N Divya Bharathi, D Ezhilarasi, RB Sangavi

Journal of Physics: Conference Series 1362 (1), 012012, 2019

The overall percentage of child abusements filed nowadays in the world is about 80%, out of which 74% are girl children and the rest are boys. For every 40 seconds, a child goes missing in this world. Children are the backbone of one's nation, if the future of children was affected, it would impact the entire growth of that nation. Due to the abusements, the emotional and mental stability of the children gets affected which in turn ruins their career and future. These innocent children are not responsible for what happens to them. So, parents are responsible for taking care of their own children. But, due to economic condition and aims to focus on their child's future and career, parents are forced to crave for money. Hence, it becomes difficult to cling on to their children all the time. In our system, we provide an environment where this problem can be resolved in an efficient manner. It makes parents to easily monitor their children in real time just like staying beside them as well as focusing on their own career without any manual intervention.

ARTICLE:22

**IoT Based Shrewd Monitoring Framework for Children Safety**

KP Revathi, T Manikandan

ECS Transactions 107 (1), 13967, 2022

system, we have developed a smart watch that can be used to locate missing or lost children and also track the child movements outside from the home as well as for facilitating women safety. Here the user itself can create his own circle in a mobile app with some radius of distance according to their comfort. When the person is out of the location, which means out of the radius, immediately the message has been sent to the emergency contacts which are already selected before by the user in the mobile app. This process can be controlled by the end user. If the user hurts in any case, it will send the alert messages to the pre-elite contacts. GPS (Global Positioning System) is employed to urge the position of a widget in terms of

latitude and meridian. Latitude and meridian values are extracted from NMEA sentences. In our system, GPS helps to send the latitude and meridian values
to the list of contacts elite by the user, once the user is not within the range of the circle. This can also be used for children as well, but when it comes to children, the complete process will be done by their parents. The app will be under parental control and they create the radius of their children to know his presence or location. This device gives the solution for knowing their location faster and facilitates to take the necessary action immediately.

ARTICLE:23

***Low-cost flow-based security solutions for smart-home IoT devices***

Arunan Sivanathan, Daniel Sherratt, Hassan Habibi Gharakheili, Vijay Sivaraman, Arun Vishwanath

2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 1-6, 2016 The rapid growth of Internet-of-Things (IoT) devices, such as smart-bulbs, smoke-alarms, webcams, and health-monitoring devices, is accompanied by escalating threats of attacks that can seriously compromise household and personal safety. Recent works have advocated the use of network-level
solutions to detect and prevent attacks on smart-home IoT devices. In this paper we undertake a deeper exploration of network-level security solutions for IoT, by comparing flow-based monitoring with packet-based monitoring approaches. We conduct experiments with real attacks on real IoT devices to validate our flow-based security solution, and use the collected traces as input to simulations to compare its processing performance against a packet-based solution. Our results show that flow-based monitoring can achieve most of the security benefits of packet-based monitoring, but at dramatically reduced processing costs. Our study informs the design of future smart-home network-level security solutions.

ARTICLE:24

**Context-sensitive policy based security in internet of things**

Prajit Kumar Das, Sandeep Narayanan, Nitin Kumar Sharma, Anupam Joshi, Karuna Joshi, Tim Finin

2016 IEEE International Conference on Smart Computing (SMARTCOMP), 1-6, 2016
According to recent media reports, there has been a surge in the number of devices that are being connected to the Internet. The Internet of Things (IoT), also referred to as Cyber-Physical Systems, is a collection of physical entities with computational and communication capabilities. The storage and computing power of these devices is often limited and their designs currently focus on ensuring functionality and largely ignore other requirements, including security and privacy concerns. We present the design of a framework that allows IoT devices to capture, represent, reason with, and enforce information sharing policies. We use Semantic Web technologies to represent the policies, the information to be shared or protected, and the IoT device context. We discuss use-cases where our design will help in creating an "intelligent" IoT device and ensuring data security and privacy using context-sensitive information sharing policies.

ARTICLE:25

**Internet of Things for education:**
A smart and secure system for schools monitoring and alerting
Kashif Naseer Qureshi, Ayesha Naveed, Yamna Kashif, Gwanggil Jeon
Computers & Electrical Engineering 93, 107275, 2021
The education system is one of the mechanisms and aspiration to build the society and contribute to human capital, well-being, and wealth. Security and privacy concerns in the educational organization is always significant due to various violent and terrorist activities. Technologies have been adopted for smart learning systems to improve the learning experience whereas security has been neglected inside or outside the institutions. The new integrated technologies have been adopted by using smart monitoring and sensing devices. The main objective of this paper is to analyze the Internet of
Things (IoT) solutions specially designed for schools to provide smart and secure systems for educational settings. This paper also proposes a Secure system for the Internet of Schools Things (S- IoST) for smart schools based on a new advanced communication system integrated with 5 G cellular systems, sensing technologies, intelligent transportation systems, and IoT networks. The proposed system provides a more secure alert mechanism and facilitates the users at school and during mobility to the school or home. The proposed system evaluates in terms of data delivery, time, and response alert parameters .

ARTICLE:26
**ChildPOPS: A Smart Child Pocket Monitoring and Protection System**
Fatma Hussain, Issam Damaj, Iyad Abu Doush
Smart Technologies for Smart Cities, 39-56, 2020
The advancements in Internet of things (IoT) technology is quickly transforming the world into a smart network of interoperable devices. Traditional devices are becoming ubiquitous, pervasive, connected, and wearable IoT gadgets. The purpose of this investigation is to develop a smart Child Pocket Monitoring and Protection System (ChildPOPS). ChildPOPS provides a touch of advanced lifestyle by automatically monitoring infant's health conditions, promoting safe living, and providing an easy-to-deploy system and a user-friendly interface. An IoT Development Model is used to design, represent, and analyze the system through a set of submodels. The main challenges that the proposed system addresses include supporting accurate physiological parameter measurements, remote sensing, and correct detection. This chapter includes studying challenges, such as accurately using the device and the training needed by the users—as related to the adoption of such a modern tool by the target human subjects.

ARTICLE:27
**IoT based smart school bus monitoring and notification system**
Judy Thyparampil Raj, Jairam Sankar
2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 89-92, 2017
It is important for every school to have a trustworthy and secure transportation service to ensure the safety of the students. It helps the school administration to effectively manage their bus fleet and potentially reduce mishaps. This is where vehicle monitoring takes effect. The proposed system

provides real time information about various parameters of the vehicle like the location, the route, the speed, the list of passengers, the adherence of drivers to schedule and much more. The system further allows the parents to be notified when their ward alights or boards the bus. In this system, we make use of RFID and GPS technologies and connect them to a remote server over WiFi using an ESP8266 microcontroller. An Ublox 6M GPS module is used to find the current geographic coordinates of the vehicle's location as well as the speed it is going at. An MFRC522 RFID reader identifies each student as they board or alight the vehicle by reading the id from their RFID tags. The system uses the ESP8266 to upload the information from the peripherals to a database in the web server. The information can be accessed by the parents through a mobile application and this helps them track their wards effectively

ARTICLE:28

**Network-level security and privacy control for smart-home IoT devices**

Vijay Sivaraman, Hassan Habibi Gharakheili, Arun Vishwanath, Roksana Boreli, Olivier Mehani

2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob), 163-167, 2015

The increasing uptake of smart home appliances, such as lights, smoke-alarms, power switches, baby monitors, and weighing scales, raises privacy and security concerns at unprecedented scale, allowing
legitimate and illegitimate entities to snoop and intrude into the family's activities. In this paper we first illustrate these threats using real devices currently available in the market. We then argue that as more such devices emerge, the attack vectors increase, and ensuring privacy/security of the house becomes more challenging. We therefore advocate that device-level protections be augmented with network-level security solutions, that can monitor network activity.

ARTICLE:29

**A capability-based security approach to manage access control in the internet of things**

Sergio Gusmeroli, Salvatore Piccione, Domenico Rotondi

Mathematical and Computer Modelling 58 (5-6), 1189-1205, 2013

Resource and information protection plays a relevant role in distributed systems like the ones present in the Internet of Things (IoT). Authorization frameworks like RBAC and ABAC do not provide scalable, manageable, effective, and efficient mechanisms to support distributed systems with many interacting services and are not able to effectively support the dynamicity and scaling needs of IoT contexts that envisage a potentially unbound number of sensors, actuators and related resources, services and subjects, as well as a more relevance of short-lived, unplanned and dynamic interaction patterns. Furthermore, as more end-users start using smart devices (e.g. smart phones, smart home appliances, etc.) the need to have more scalable, manageable, understandable and easy to use access control mechanisms increases. This paper describes a capability based access control system that enterprises, or even individuals, can use to manage their own access control processes to services and information.

ARTICLE:30

**IoT-BBMS: Internet of Things-based baby monitoring system for smart cradle**

Waheb A Jabbar, Hiew Kuet Shang, Saidatul NIS Hamid, Akram A Almohammedi, Roshahliza M Ramli,
Mohammed AH Ali
The current number of working mothers has greatly increased. Subsequently, baby care has become a daily challenge for many families. Thus, most parents send their babies to their grandparents' house or to baby care houses.