IOT security by application of internal fail-safe mechanisms.

A study of established methodologies.

Avik Mitra
Undergraduate, School of Computer Science and Engineering
VIT University.
Vellore, India.
mitraavik1@gmail.com

S. Chandramaouli
Undergraduate, School of Computer Science and Engineering
VIT University.
Vellore, India
c.maouli2017@gmail.com

Vaidhyanathan C
Undergraduate, School of Computer Science and Engineering
VIT University.
Vellore, India.
vaidhyanathan8460@gmail.com

Rachit Trilok
Undergraduate, School of Computer Science and Engineering
VIT University.
Vellore, India
rachittrilok82@gmail.com

Sambhav Jain
Undergraduate, School of Computer Science and Engineering
VIT University.
Vellore, India.
coolsam248@gmail.com

***Abstract*— The advent and integration of Internet of Things into various industries has caused a boom in the demand of IoT based services in modern workplace as well as homes and other related services.**

It is imperative that with the inclusion of such services into the work environment, opens the said environment susceptible to various attacks and threats from multiple sources. An IoT based service might be attacked through false identities, open networks, compromised administrator credentials among other equally severe factors.

To be aware and alert of such security threats to the system, precautions based on the management of security events within IoT scenarios in order to accurately identify suspicious activities is applicable.

Applicable operating system security in these aspects is essential to safeguard user information an protect the user as well as related entities from any kind of data leak, loss or harm in any other manner.

***Index Terms*—Internet of Things, false identity, Operating systems, security, attack, leak, open networks, compromised administrator.**

I. Introduction

The emergence of new low power IoT networks in which leaf nodes have native IPv6 connectivity and the grown awareness for data protection of IoT devices require leaf nodes to provide a higher level of security, similar to the level of a standard computer system. Especially in terms of energy consumption and device cost, the intensive cryptographic operations of well-known computer security algorithms are a big challenge for resource constrained devices. To face these challenges, semiconductor vendors have recently introduced new dedicated hardware, so called secure elements. These devices provide hardware accelerated support for cryptographic operations and tamper proof memory for the secure storage of cryptographically sensitive material. Further, they employ specific techniques against so-called side channel attacks.

Sancus security architecture for networked embedded devices was proposed in 2013 at the USENIX Security conference. It supports remote (even third-party) software installation on devices while maintaining strong security guarantees.

Device authentication is yet another essential security feature for Internet of Things (IoT). Many IoT devices are deployed in the open and public places, which makes them vulnerable to physical and cloning attacks. Therefore, any authentication protocol designed for IoT devices should be robust even in cases when an IoT device is captured by an adversary.

With the spread of Internet of Things' (IoT) applications, security has become extremely important. A recent distributed denial-of-service (DDoS) attack revealed the ubiquity of vulnerabilities in IoT, and many IoT devices unwittingly contributed to the DDoS attack. The emerging software-defined anything (SDx) paradigm provides a way to safely manage IoT devices.

II. Security and Privacy needs

The described technical architecture of the IoT has an impact on the security and privacy of the involved stakeholders.[1] Privacy includes the concealment of personal information as well as the ability to control what happens with this information.12 The right to privacy can be considered as either a basic and inalienable human right, or as a personal right or possession.13 The attribution of tags to objects may not be known to users, and there may not be an acoustic or visual signal to draw the attention of the object's user. Thereby, individuals can be followed without them even knowing about it and would leave their data or at least traces thereof in cyberspace. Further aggravating the problem, it is not anymore only the state that is interested in collecting the respective data, but also private actors such as marketing enterprises. Since business processes are concerned, a high degree of reliability is needed. The following security and privacy requirements are:

1. Resilience to attacks: The system has to avoid single points of failure and should adjust itself to node failures.
2. Data authentication: As a principle, retrieved address and object information must be authenticated.
3. Access control: Information providers must be able to implement access control on the data provided.
4. Client privacy: Measures need to be taken that only the information provider is able to infer from observing the use of the lookup system related to a specific customer; at least, inference should be very hard to conduct. Private enterprises using IoT technology will have to include these requirements into their risk management concept governing the business activities in general.

III. Contrasting Methods of Protection

When we are looking at an emerging technology such as Internet of Things itself we need to understand that the protection requirements for this kind of technology. Young technology like this is always open to attacks trying to exploit all fronts of the system's most basic vulnerabilities. Since the technology is still in its base form, the developers don't have the appropriate precedence or expertise on how to optimally protect the system most efficiently. This might lead to institutions with malicious intent or otherwise gaining access to data or control they are not authorized to handle. This brings us to write this paper in order to compare and contrast various security methodologies and protocols to give us a better understanding of what is best for the protection. We get an insight into the best security features available and currently and propose an idea to integrate the best systems into a culminative operating system security feature of the central IOT mechanism.

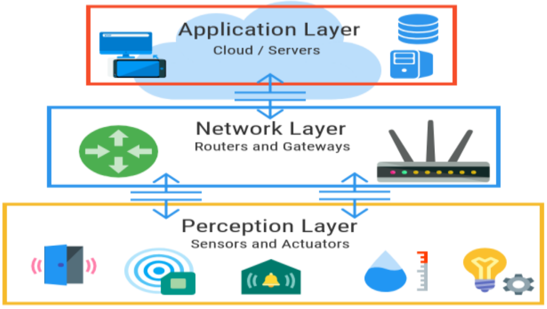
IV. Abbreviations

Short	**Elaboration**
IOT	Internet of Things
SIEM	Security information and event management
REST	Representational State Transfer
DDoS	Distributed Denial of Service
PUF	Physical Unclonable Function
SDx	Software-defined anything
IC	Integrated Circuit
TCB	Trusted Computing Base
SPEP	Security Policy Enforcement Point
SDN	Software-defined networking
TLS/SSL	Transport Layer Security/ Secure Sockets Layer

V. Internet of Things Architecture

In an IoT architecture, each layer is explained by its functions and the devices that are used in the layer. There are different beleives regarding the number oflayers in IoT. However, according to many investigators , the IoT essentially utilizes on three layers which are the Perception, Network, and the Application layer. Each layer of IoT has intrinsic security issues related with it.

1. **Perception Layer**: The perception layer is also known as the "Sensors" layer in IoT. The motive of this layer is to receive data from the environment with the help of sensors. This layer observes, collects, and processes data from sensors and then convey it to the network layer. In addition, this layer may also perform IoT node combination in local and short range networks.
2. **Network Layer**: The network layer of IoT performs the task of data routing and communication to different IoT hubs and devices over the Internet. At this layer, Internet gateways, switching, and routing devices etc. run by using some of the very modern technologies such as Wi-Fi, LTE, Bluetooth, 3G, Zigbee etc. to provide disparate network services. The network gateways serve as the negotiator between different IoT nodes by combining, filtering, and communicating data to and from different sensors.
3. **Application Layer**: The application layer assures the authenticity, integrity, and confidentiality of the data. At this layer, the intention of IoT which is the creation of smart environments is executed.



VI. Literature Surveys

This article presents a lightweight and privacy-preserving two-factor authentication scheme for IoT devices, where physically unclonable functions (PUFs) have been considered as one of the authentication factors. Security and performance analysis show that our proposed scheme is not only robust against several attacks, but also very efficient in terms of computational efficiently.[2]

To provide two-factor authentication to IoT devices, in addition to a password or a shared secret key as the first authentication factor, this paper proposes the use of physically unclonable functions as the second authentication factor.

PUFs have emerged as a promising cryptographic primitive and already gained popularity in the security domain, and their practicality has also been demonstrated in many recent works. PUFs are the result of the manufacturing process of Integrated Circuits (ICs) which introduces random physical variations into the micro-structure of an IC, making it unique. It is impossible to control these variations in the micro-structure of an IC during the manufacturing process. In addition, the outputs are derived from intrinsic characteristics of the PUF's physical elements and are therefore difficult to predict and almost impossible to clone. In this regard, PUF uses their internal structure to provide a one-way function that cannot be duplicated. The fact that PUFs are hard to predict but easy to construct and evaluate makes them a good choice for use as a security primitive for IoT devices.

The emerging software-defined anything (SDx) paradigm provides a way to safely manage IoT devices. The proposed framework consists of a controller pool containing SD-IoT controllers, SD-IoT switches integrated with an IoT gateway, and IoT devices. We then propose an algorithm for detecting and mitigating DDoS attacks using the proposed SD-IoT framework, and in the proposed algorithm, the **cosine similarity** of the vectors of the packet-in message rate at boundary SD-IoT switch ports is used to determine whether DDoS attacks occur in the IoT.[3]

These networking devices have no user interface, no security protocol, and no computing and storage capacity to enable firewalls and diagnostic tools; moreover, they cannot directly connect to the Internet via Wi-Fi. These vulnerabilities represent temptation not only for organizations that want to collect data to achieve intelligent management and digital evidence but also for those who want to disseminate DDoS attacks or other malicious intrusions. Once a DDoS attack is successful, it may threaten the safety of human life and even directly or indirectly cause death and destruction. In recent years, many examples have shown that IoT is vulnerable to viruses. Recent DDoS attacks have revealed that loopholes are ubiquitous in IoT, which is still in the initial stage. Without security precautions, the vast majority of IoT devices may unknowingly become accomplices to DDoS attacks.

The software-defined anything (SDx) paradigm addresses the above-mentioned problems. SDx includes software- defined radio (SDR), software-defined networking (SDN), software-defined data centers (SDDC), software defined infrastructure (SDI),and the software-defined world (SDW). SDN is undoubtedly the most recognized technology, and its core technology is the separation of the control plane and data plane in the network. It realizes flexible control of network traffic and provides a good platform for the innovation of core networks and applications.

The key feature of SD-IoT is that it decouples network control and forwarding functions. The SD-IoT controller in the control layer is responsible for the logic centralized control of IoT. The SD-IoT switches, e.g., two-layer or three-layer switches, routers, base stations and wireless access points, only act as the data layer of IoT, and they only perform flow forwarding. Using a programming interface (such as REST) provided by the SD-IoT controller, users can interact directly with IoT devices, configure the edge computing, analyze the environment and deploy security control. This decoupling avoids potential operation failure and service interruption, ensures the continued availability of IoT devices, prevents unauthorized access to peripheral devices, monitors and controls changes to the Internet of devices, detects legitimate and malicious traffic patterns on IoT devices, and ultimately reduces the risks managed by IoT security.

This paper describes a general framework for SD-IoT composed of an SD-IoT controller pool with controllers, SD-IoT switches integrated with the IoT gateway, and terminal IoT devices. An algorithm is proposed for detecting and mitigating DDoS attacks with the proposed SD-IoT framework. In the proposed algorithm, the threshold value of the cosine similarity of the vectors of the packet-in rate at the ports of the SD-IoT boundary switches is obtained; the threshold value is used to determine whether a DDoS attack has occurred, find the real DDoS attacker, and block the DDoS attack at the source. Finally, the simulation results show that the proposed algorithm can find the IoT device from which a DDoS attack is launched within a shorter time period, quickly handle and mitigate the DDoS attack, and ultimately improve the unveiled glaring vulnerabilities in IoT, in which the terminal devices have computational and memory requirement constraints.

Sancus security architecture for networked embedded devices was proposed in 2013 at the USENIX Security conference. It supports remote (even third-party) software installation on devices while maintaining strong security guarantees. More specifically, Sancus can remotely attest to a software provider that a specific software module is running uncompromised and can provide a secure communication channel between software modules and software providers. Software modules can securely maintain local state and can securely interact with other software modules that they choose to trust.[4]

Computing devices and software are omnipresent in our society, and society increasingly relies on the correct and secure functioning of these devices and software. Two important trends can be observed. First, network connectivity of devices keeps increasing. More and more (and smaller and smaller) devices get connected to the Internet or local ad-hoc networks. Many consumer products contain embedded technology to have Internet connectivity. This Internet of Things (IoT) is estimated to grow to an astonishing number of 26 billion units by 2020. Second, more and more devices support extensibility of the software they run – often even by third parties different from the device manufacturer or device owner. However, these two factors also have a significant impact on security threats. The combination of connectivity and software extensibility leads to malware threats.

However, for low-end, resource-constrained devices, no effective low-cost solutions are known. Many embedded platforms lack standard security features present in high-end processors, such as privilege levels or advanced memory management units that support virtual memory. Over the past few years, researchers have been exploring alternative security architectures for

low-end networked devices. For instance SMART, a simple and efficient hardware software primitive to establish a dynamic root of trust in an embedded processor, and a simple program counter-based memory access control system to isolate software components.

Sancus was first proposed in 2013 at the USENIX Security

Conference as a security architecture that supports secure third-party software extensibility for a network of low-end processors with a hardware-only Trusted Computing Base (TCB).

This paper refers to resource constrained devices as leaf nodes and understands them as a battery powered electronic device which is controlled by a microcontroller unit (MCU). The native IPv6 connectivity offers many opportunities such as service discovery, end-to-end security and transparent routing down to the leaf node. However, due to the missing gateway and straightforward accessibility, the leaf node is exposed to attacks from the outside world.[5]

Furthermore, the leaf node can be directly connected to the IT infrastructure and therefore may serve as a simple entry point for attackers. As a result, the required security level for a leaf node is much higher in such IoT networks. The challenge is to leverage the elaborate, well-known computer security, which otherwise would be provided by a gateway, to the resource constrained device without dramatically increasing the power consumption nor the cost with regard to memory sizes and required processor performance.

To face these challenges, semiconductor vendors have recently introduced dedicated hardware devices, so called secure elements.

Secure elements execute cryptographic operations in hardware, which allows for fast and energy efficient execution of cryptographic algorithms. Furthermore, secure elements provide tamper proof memory for secure storage of cryptographic material.

These features allow the leaf node to provide a high security level and to be an authentic and secure member of an IT infrastructure.

The paper[6] uses the concept of APIs to build an architecture establishing end to end security in IoT platforms. Probes which connect the external environment to IoT Edge device are registered in IoT probes registry and the data is routed to the destination using Security Policy Enforcement Point (SPEP). The data to be routed is subject to algorithms which encrypt it. This paper has shed light into the challenges of building such infrastructures. The presented solutions are configurable, scalable and intelligent, leveraging on existing Big Data infrastructures. The paper has also described a prototype implementation to demonstrate the concept.

The research paper[7] goes into more detail on the APIs introduced by the previous paper discussed by explaining the need for a middleware. REST APIs are configured using JSON which handles an pivotal role in response management in security. Middleware successfully assists IoT development by exposing REST API and providing an interface to the user to register their IoT devices and then securely accessing data collected by the device.

The paper[8] utilizes Etherium(virtual currency derived from an existing bit coin) as a DB server instead of using the conventional general DB server by utilizing the existing IoT platform server, Mobius, and additionally the Ethernet network. The IoT device information and the sensor data are stored in a block chain of the etherium network to make it more secure and easy to manage.

SDN Enabled Secure IoT Architecture

The paper[9] focuses on proposing a security solution for IoT network infrastructure. Security architecture uses SDN to provide authentication and authorization services to IoT network infrastructure. SDN-IoT security architecture allows communication for IoT devices that have been authenticated (IoT Authentication Authority) and whose requests for network services are authorized against a set of policies specified in PbSA which determines whether the security constraints have been met. The separation between control and data planes has been achieved using the SDN architecture whereby the ability to control access is managed separately from the transmission of data and the communications between the IoT devices are virtualized using overlays that represent logical paths over a physical network.

Following up on the previous paper, this paper seeks to integrate SDN with cloud computing.[10] Each SDN controller authenticates and manages devices that belong to its domain by registering them with their identities and addresses for identification and forwarding mechanism, devices in the same domain communicate using their SDN domain controllers or another SDN controller in case the one associated is unavailable. In case a node wants to establish a communication, the authentication is performed by the associated SDN domain controllers that share security rules among them while messages encryption and decryption are performed partially on the node using symmetric methods that are suitable for constrained nodes and then sent to the RCS deployed in the cloud to complete the encryption using asymmetric methods.

The view of the research articles[11][12][13][14] are mostly that the main vulnerability of IoT based system is illegal access to the first node. Authentication is widely suggested as the ideal solution to this matter. To protect confidentiality of the information, encryption is suggested but the perception layer can consume a very large amount of resources if heavy encryption is used. So, the challenge presented is to use strong but relatively lightweight encryption and crystallographic methods to preserve economy of resource usage.
In the Network layer existing communication security mechanisms are difficult to be applied. Identity authentication is a kind of mechanism to prevent the illegal nodes, and it is the premise of the security mechanism, confidentiality and integrality are of equal importance, thus we also need to establish data confidentiality and integrality mechanism. Besides distributed denial of service attack (DDoS) is a common attack method in the network and is particularly severe in the internet of thing, so to prevent the DDOS attack for the vulnerable node is another problem to be solved in this layer.

Encryption Mechanism:

In the traditional network layer by-hop encryption mechanism is adopted, in this way the information is encrypted in the transmission process, but it needs to keep plaintext in each node through the decryption and encryption operations. Meanwhile in the traditional application layer encryption mechanism is end-to-end encryption, that is, the information only is explicit for the sender and the receiver, and in the transmission process and forwarding nodes it will be always encrypted. In the IoT network layer and application layer connect so closely, so we have to choose between by-hop and end-to-end encryption. If we adopt by-hop encryption, we can only encrypt the links which need be protected, because in the network layer we can apply it to all business, which make different applications safely implemented. In this way, security mechanism is transparent to the business applications, which gives the end users convenience. In the meantime, this brings the features of the by-hop full play, such as low latency, high efficiency, low cost, and so on. However, because of the decryption operation in the transmission node, using by-hop encryption each node can get the plaintext message, so by-hop encryption needs high credibility of the transmission nodes . Using the end-to-end encryption, we can choose different security policy according to the type of business, thus it can provide high level security protection to the high security requirements of the business. However, end-to-end encryption cannot encrypt the destination address, because each node determines how to transmit messages according to the destination address, which causes it cannot hide the source and the destination of the message being transmitted and bring about malicious attacks. Through the above analysis, we can draw a conclusion: when the security requirement of some business is not very high, we can adopt by-hop encryption protection; when the business needs high-security, then end-to-end encryption is the first choice.

Communication Security:

At first in communication protocols there are some solutions being established, these solutions can provide integrity, authenticity, and confidentiality for communication, for example: TLS/SSL or IPSec. TLS/SSL is designed to encrypt the link in the transport layer, and IPSec is designed to protect security of the network layer, they can provide integrity, authenticity, and confidentiality in each layer.
And the needs of privacy also have been come up with but unfortunately, are not in wide use.
Then communication security mechanisms are also seldom applied nowadays. Because in the IoT small devices are less processing power, this leads that communication security is often weak. Meanwhile in the IoT, the core network is always the current or next-generation Internet, most of the information will be transmitted through the Internet. So DDoS still exists and is a very severe problem. These botnets and DDoS attacks will destroy the availability of communication. When larger-scale or organized DDoS attacks happen, how to do the disaster recovery is highly significant, so we need pay more attention to researching better preventive measures and disaster recovery mechanisms.

Protecting Sensor Data:

The integrity and authenticity of sensor data is a main security focus, and confidentiality of sensor data is a lower demand because when an attacker can just place its own sensor physically near, he can sense the same values. So, at the sensor itself the confidentiality need is relatively low.

The other main research target in sensors is privacy, and privacy is also a major problem. We should adopt the mechanisms to protect the privacy of humans and objects in the physical world. Most times people are often unaware of sensors in their life, so we need to set up regulations to preserve the privacy of people. In the literature , several guidelines are given to solve this problem in the design phase: at first users must know that they are being sensed, the second users must be able to choose whether they are being sensed or not, the third users must be able to remain anonymous. When the user has no realization of these guidelines, that regulations must be made.

Security Information and Event Management (SIEM) is the state-of-the-practice to address the complexity underlying the collection and normalization of diverse data sources for security analysis. SIEM is the *core component* of any typical Security Operations Center (SOC), i.e., the centralized response team dealing with security incidents within an organization [16]; however, we observe that integrating a SIEM in a given system is far from being seamless.[16]

Security Information and Event Management (SIEM) is an approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system.

The underlying principles of every SIEM system is to aggregate relevant data from multiple sources, identify deviations from the norm and take appropriate action. For example, when a potential issue is detected, a SIEM might log additional information, generate an alert and instruct other security controls to stop an activity's progress.[17]

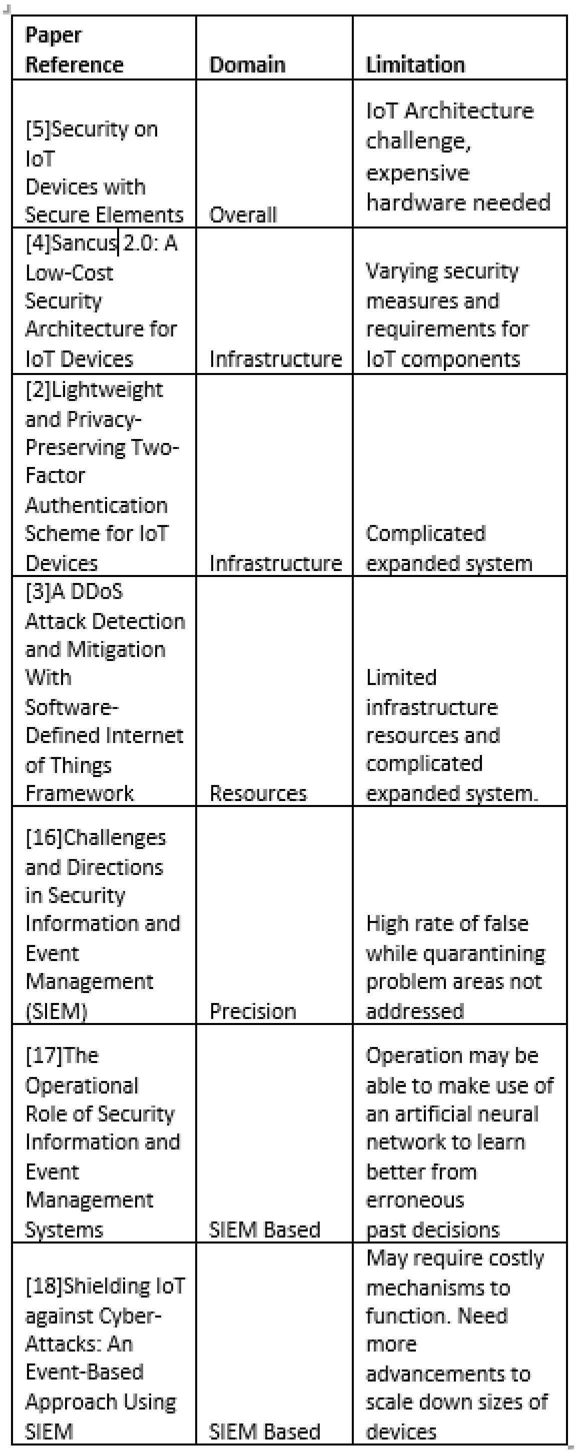
At the most basic level, a SIEM system can be rules-based or employ a statistical correlation engine to establish relationships between event log entries. Advanced SIEMs have evolved to include user and entity behaviour analytics (UEBA) and security orchestration and automated response (SOAR).

Inclusion of SIEM into the operating system of an IoT based device would help raise red flags and possibly kill activities that might cause data loss and other kinds of issues. This would help prevent any kind of activity in progress that is detrimental to the functioning of the system and kill it before it can do any further, major harm to the overall functioning of the linked peripherals and cause additional privacy breaches to the said system.[18]

The security operations center (SOC) is a centralized unit tasked with real-time monitoring and identification of security incidents. Security information and event management (SIEM) systems are an important tool used in SOCs; they collect security events from many diverse sources in enterprise networks, normalize the events to a common format, store the normalized events for forensic analysis, and correlate the events to identify malicious activities in real time.[17, 18]

Services like such are provided by IBM QRadar Security Information and Event Management (SIEM) helps security teams accurately detect and prioritize threats across the enterprise, and it provides intelligent insights that enable teams to respond quickly to reduce the impact of incidents.[20] By consolidating log events and network flow data from thousands of devices, endpoints and applications distributed throughout your network, QRadar correlates all this different information and aggregates related events into single alerts to accelerates incident analysis and remediation. QRadar SIEM is available on premises and in a cloud environment.

LIMITATIONS OF COMPILED WORK



Paper Reference	Domain	Limitation
[5]Security on IoT Devices with Secure Elements	Overall	IoT Architecture challenge, expensive hardware needed
[4]Sancus 2.0: A Low-Cost Security Architecture for IoT Devices	Infrastructure	Varying security measures and requirements for IoT components
[2]Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices	Infrastructure	Complicated expanded system
[3]A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework	Resources	Limited infrastructure resources and complicated expanded system.
[16]Challenges and Directions in Security Information and Event Management (SIEM)	Precision	High rate of false while quarantining problem areas not addressed
[17]The Operational Role of Security Information and Event Management Systems	SIEM Based	Operation may be able to make use of an artificial neural network to learn better from erroneous past decisions
[18]Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM	SIEM Based	May require costly mechanisms to function. Need more advancements to scale down sizes of devices

CONCLUSION

IT and control systems manufacturers are seizing the opportunity of having new novel hardware devices as the "Internet of Things" begins to scale up. As the number of devices continues to increase, more automation will be required for both the consumer (e.g. home and car) and industrial environments. As automation increases in IoT control systems, software and hardware vulnerabilities will also increase. In the near term, data from IoT hardware sensors and devices will be handled by proxy network servers (such as a cellphone) since current end devices and wearables have little or no built-in security. The security of that proxy device will be critical if sensor information needs to be safeguarded. The number of sensors per proxy will eventually become large enough so that it will be inconvenient for users to manage using one separate app per sensor. This implies single appls with control many "things," creating a data management (and vendor collaboration) problem that may be difficult to resolve. An exponentially larger volume of software will be needed to support the future IoT. The average number of software bugs per line of code has not changed, which means there will also be an exponentially larger volume of exploitable bugs for adversaries. Until there are better standards for privacy protection of personal information and better security guidelines on communication methods and data/cloud storage, security of wearable and other mobility devices will remain poor. More work needs to be spent on designing IoT devices before too many devices are built with default (little or no) security. Physical security will change as well. As self-healing materials and 3D printers gain use in industry, supply-chain attacks could introduce malicious effects, especially if new materials and parts are not inspected or tested before use.

The main benefits of autonomous capabilities in the future IoT is to extend and complement human performance. Robotic manufacturing and medical nanobots may be useful; however, devices (including robots) run software created by human. The danger of the increased vulnerabilities is not being addressed by security workers at the same rate that vendors are devoting time to innovation. Consider how one might perform security monitoring of thousands of medical nanobots in a human body.

The ability to create secure IoT devices and services depends upon the definition of security standards and agreements between vendors. ISPs and telecommunication companies will control access to sensor data "in the cloud" and they cannot provide 100% protection against unauthorized access. IoT user data will be at risk. Diversity of the hardware and software in the future IoT provides strong market competition, but this diversity is also a security issue in that there is no single security architect overseeing the entire "system" of the IoT. The "mission" of the entire IoT "system" was not pre-defined; it is dynamically defined by the demand of the consumer and the response of vendors. Little or no governance exists and current standards are weak. Cooperation and collaboration between vendors is essential for a secure future IoT, and there is no guarantee of success.

Acknowledgment

We would like to thank our Operating Systems faculty, Prof. Rahul Raman, dept. CSE, VIT University, Vellore, for giving us the much needed encouragement to transform our research work into a survey paper. We would also like to thank other support staff who helped us champion through this endeavor and successfully conclude our work.

References

[1] R. H. Weber, "Internet of things – new security and privacy challenges," Computer Law & Security Review, vol. 26, pp. 23-30, 2010.

[2] Prosanta Gope and Biplab Sikdar, Senior Member, IEEE, "Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices", IEEE INTERNET OF THINGS JOURNAL, vol. xx, no. x, xxx 2018

[3] DA YIN1 , LIANMING ZHANG 1 , AND KUN YANG 2 , (Senior Member, IEEE), "A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework", IEEE Access, Special section on security and trusted computing for industrial IOT.

[4] Noorman, Job & Freiling, Felix & Van Bulck, Jo & Mühlberg, Jan & Piessens, Frank & Maene, Pieter & Preneel, Bart & Verbauwhede, Ingrid & Götzfried, Johannes & Müller, Tilo. (2017)., "Sancus 2.0: A Low-Cost Security Architecture for IoT Devices.", ACM Transactions on Privacy and Security. 20. 1-33. 10.1145/3079763.

[5] Tobias Schläpfer, Andreas Rüst Zurich University of Applied Science (ZHAW) Institute of Embedded Systems (InES), "Security on IoT Devices with Secure Elements", Embedded World 2019 conference.

[6] A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke and N. Kefalakis, "Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data : Towards End-to-End Security in IoT Systems," *2019 Global IoT Summit (GIoTS)*, Aarhus, Denmark, 2019, pp. 1-6. doi: 10.1109/GIOTS.2019.8766407

[7] H. Garg and M. Dave, "Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware," *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Ghaziabad, India, 2019, pp. 1-6.
doi: 10.1109/IoT-SIU.2019.8777334

[8] J. H. Jeon, K. Kim and J. Kim, "Block chain based data security enhanced IoT server platform," *2018 International Conference on Information Networking (ICOIN)*, Chiang Mai, 2018, pp. 941-944.
doi: 10.1109/ICOIN.2018.8343262

[9] K. K. Karmakar, V. Varadharajan, S. Nepal and U. Tupakula, "SDN Enabled Secure IoT Architecture," *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, Arlington, VA, USA, 2019, pp. 581-585.

[10] R. Djouani, K. Djouani, F. Boutekkouk and R. Sahbi, "A Security Proposal for IoT integrated with SDN and Cloud," *2018 6th International Conference on Wireless*

Networks and Mobile Communications (WINCOM), Marrakesh, Morocco, 2018, pp. 1-5. doi: 10.1109/WINCOM.2018.8629727

[11] Suo, Hui & Wan, Jiafu & Zou, Caifeng & Liu, Jianqi. (2012), " Security in the Internet of Things: A Review." Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012. 3. 10.1109/ICCSEE.2012.373.

[12] Siddiqui T, Alazzawi SSB (2018), "Security of Internet of Things." Int J Appl Sci Res Rev Vol.5 No.2:8

[13] Dr. Yusuf Perwej, Firoj Parwej, Mumdouh MirghaniMohamed Hassan, Nikhat Akhtar, "The Internet-of-Things (IoT) Security : A Technological Perspectiveand Review ", International Journal of ScientificResearch in Computer Science, Engineering andInformation Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 1, pp. 462-482, January-February 2019.

[14] The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved by Wei Zhou, Yuqing Zhang, and Peng Liu, Member, IEEE

[15] Blowers, Misty & Iribarne, Jose & Colbert, Edward & Kott, Alexander. (2016). In Conclusion: The Future Internet of Things and Security of Its Control Systems. 10.1007/978-3-319-32125-7_16.

[16] M. Cinque, D. Cotroneo and A. Pecchia, "Challenges and Directions in Security Information and Event Management (SIEM)," *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Memphis, TN, 2018, pp. 95-99. doi: 10.1109/ISSREW.2018.00-24

[17] S. Bhatt, P. K. Manadhata and L. Zomlot, "The Operational Role of Security Information and Event Management Systems," in *IEEE Security & Privacy*, vol. 12, no. 5, pp. 35-41, Sept.-Oct. 2014.
doi: 10.1109/MSP.2014.103

[18] Daniel Díaz López, María Blanco Uribe, Claudia Santiago Cely, et al., "Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM," Wireless Communications and Mobile Computing, vol. 2018, Article ID 3029638, 18 pages, 2018. https://doi.org/10.1155/2018/3029638.

[19] [URL] Security Information and Event Management (SIEM), Retrieved September 21st 2019, from: https://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

[20] [URL] IBM QRadar, Security Intelligence, (October 18, 2019) from: https://www.ibm.com/security/security-intelligence/qradar? …………………………………………..