Security Solution for the IOT Devices

Dr. Gorti VNKV Subbarao

Abstract- As the internet is available widely with low cost to connect with the devices day by day. Almost all electronic devices are coming to the market with wi-fi capabilities and sensors built into them, even technology costs also coming down. All of these devices are forming Network by accessing the internet through their wi-fi capabilities. These are creating a perfect IOT storm like smart phones are becoming rocks and penetrating everywhere so the sky is the limit for them. As these all are in the hands of everybody, there is obviously security threats. In this paper, all the possible threats are addressing with possible solutions occurring in these IoT devices. Suggested the Homomorphic Encryption scheme for security in IoT devices.

Keywords: internet of things, homomorphic encryption scheme, encryption, enhanced homomorphic encryption.

I. Introduction

As the internet is available widely with low cost to connect with the devices day by day. Almost all electronic devices are coming to the market with wi-fi capabilities and sensors built into them, even technology costs also coming down. All of these devices are forming Network by accessing internet through their wi-fi capabilities. These are creating a perfect IoT storm like smart phones are becoming rocks and penetrating everywhere so the sky is the limit for them. As these all are in the hands of everybody, there is obviously security threats [4]. In this paper, all the possible threats are addressing with possible solutions occurring in these IoT devices.

The Internet of Things (IoT) is the collection of many things to many people. Everything from new applications generated, such as smart cities/townships or autonomous vehicles/devices to massive sensor networks for monitoring environmental elements or industrial systems or procedures

Another way we can define IoT as a system of interrelated computing systems or devices includes electrical, mechanical, digital machines and the objects includes animals or human being that are provided with unique identifiers and they will have the capability of transferring data between the devices or objects over the network without demanding interaction between them[1].

In the IoT the things may be a person, animal or device like a human brain means a farm animal with a biochip, an automobile or device having a sensors in it to alert the driver when tire pressure is not upto the mark or any other natural or artificial object assigned with an IP address and that can be able to send data over a network to destination.

As we know that this field IoT is continually growing with advancements in core technologies, hardware and software enhancements with generated products. So the internet of things making industry grow fast with these latest components.

II. History of Iot

Kevin Ashton, Auto-ID Center co-founder at MIT, mentioned the term the internet of things in his presentation 1999[2]. He wants to bring radio frequency ID (RFID) to the attention senior management, Ashton named his presentation "Internet of Things" to incorporate the new trend of the internet. Another MIT professor Neil mentioned in his book indirectly that Things Start to think for interacting with each other.

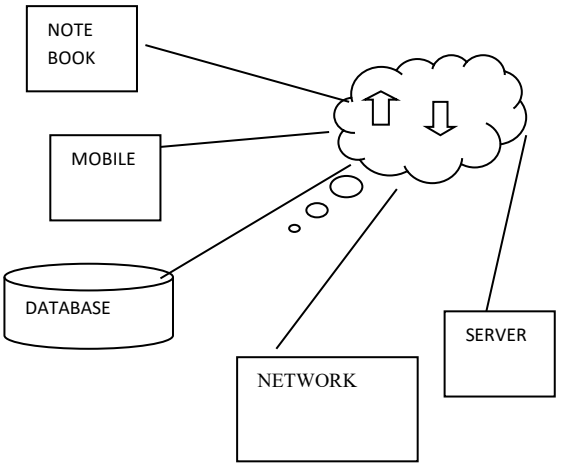
IoT includes, the convergence of wireless technologies, micro electro mechanical systems, micro services and the internet. The convergence has helped to fill the gap between operational technology and information technology, enabling unstructured machine-generated data to be analyzed for future predictions or steps.

We have seen in the early 1980s the first internet appliance, a Coke machine at Carnegie Mellon University. Using the web, programmers understand the status of the machine whether there would be a cold drink available or not [3].

III. Internet of Things Working Style

An IoT ecosystem consists of internet-enabled wise gadgets that use embedded processors, sensors, conversation hardware to acquire, store, act on gathered data. IoT gadgets share the sensed data by connecting to an IoT gateway to analyze or transfer it to the cloud to be analyzed. Every so often, those devices communicate with each other connected devices and act on the facts each other. These devices perform maximum of the works without human help except to set them up, deliver them commands or get admission to the records[6].The main factors like connectivity, networking and communication protocols used with these web-enabled devices depends on the specific IoT applications.

Author: Associate Professor, CSE, Keshav Memorial Institute of Technology, Narayanaguda, Hyderabad, Telangana, India.
e-mail: gvnkvsubbarao@yahoo.com



IV. The IOT Impact on The Industry

In coming days we may understand, "Anything that could be connected, would be connected." We also understand the importance of connected devices talking to each other. Take the following contexts to understand well, suppose you are on the way to a meeting, your car could have access to your route map and knows the best route to take. If the traffic is heavy your car might send a message to the other party informing them that you will be late. your alarm clock wakes up you at 5 a.m. and then give signal to your coffee maker[7]. Your store equipment knew when it was running low and automatically order to supplier. The wearable device you used in the workplace could alert you when and where you should be active and productive and shares that information with other devices also connected to you.

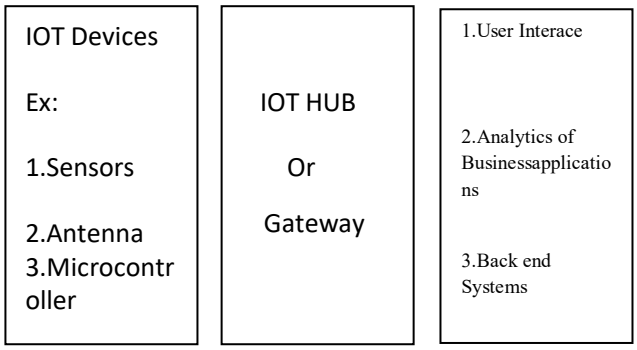
The Internet of Things is the upcoming digital transformation. Digitizing things - from bulbs, watches to industrial equipment - creates new opportunities for industry to increase operational productivity, enhance users experiences, and increases web revenue. With web IoT, we can manage billions of devices, run analytics and machine learning, and take actions to make better steps [8]. AWS offers the most complete precxedure, from edge to cloud, for both Industrial IoT and the Connected Home. For IIoT, industry community can optimize operations in the areas of predictive quality and maintenance or remote monitoring. In Home network, engineers can bring new functionalities to smart devices, namely, interconnectivity, and machine learning, security.

V. Categories of Internet of Things

IoT classified into The internet and the things, with several subcategories.

1. Internet
   Hard Infrastructure
   API Cloud Services
   Cloud Scale Platforms
2. Things
3. *Sensors*
4. Actuators
5. Services

Collect data → Collect and Transfer date → analaya data and take step.



VI. IOT Benefits and Applications

Number of benefits to organizations, enabling them to:

- Overall business steps will be managed.
- Customer experiences will be improved.
- Time and money will be saved.
- Employee productivity increases.
- Business models can be integrate and adapt.
- Business decisions can be made better.
- Increases revenue.

VII. Possible Threats in the IOT Devices and Challenges

As per the survey there are 50 billion IoT connected devices by the year 2025. So that IoT devices will soon play vital role in our daily lives. Modern households are going to connect to the internet — sharing information with each other and often sending reports and notifications to your phone [9]. We are observing the same in the mobile application market for these devices. Some are even interpreting that these new IoT mobile applications may take over the cell phone and tablet market in the next coming years.

Devices with the Internet of Things concept may be required, but there is huge security risks involved in it. Recently, there has been a rise in IoT devices being hacked and added to small files in order to carry out malicious attacks. Sensitive data in the IoT devices may be stolen by hackers simply. Sensitive data with weak infrastructure makes IoT devices extremely target for hackers. The first thing IoT users should avoid the default passwords to keep their data, and homes, safe. Many routers and other devices have been attacked because of default passwords and simple IoT devices are following suit. Surprisingly large amount of first grade professionals are using these default passwords, which only makes them target. Mostly hacker needs to

© 2019 Global Journals

study a manual in order to take advantage of IoT devices on the market, if they use to create a strong password, avoid using routine passwords with names, common nouns and short strings of numbers. These types of passwords are not safe easily can guess. Long, complex passwords are ideal to prevent the most basic hacking attempts. Use a special combination of letters and numbers, symbols and varying letter case in your passwords to keep your data safe.

VIII. IOT Security Challenges

A number of procedures prevent the securing of IoT devices and ensuring end-to-end security. Idea of networking appliances and other objects working together is new, security has not always been considered top most priority while design phase. As they have fast demand in market, many product designers and manufacturers shows more interested in releasing their products to market quickly, rather than embedding security features from the start [10].

A major issue identified in IoT security is the use of weak password which can lead to security breaches. Even if passwords are changed, they are often not strong enough to prevent its security.

In terms of updates, many systems only include support for a set timeframe. For legacy and new assets, security can lapse if extra support is not added in the devices. And as many IoT devices stay in the network for many years, adding security can be challenging.

IoT security is very weak because of lack of industry-accepted standards. Even though many IoT security frameworks exist, there is no single agreed-upon framework. Large companies and industry organizations may have their own specific standards [12], while certain segments, such as industrial IoT, have proprietary, incompatible standards from industry managers. The various standards makes it difficult for secure systems, even arises interoperability problem between them.

IX. Internet of Things Security Solutions to Protect Iot Systems and Devices

The challenges and design issues that affect data process in IoT systems and devices.

1. Network longevity
2. Responsiveness
3. Fault tolerance
4. Scalability
5. Heterogeneity
6. Self-configuration
7. Privacy and security
8. Data reporting
9. Connectivity and coverage
10. Delay

X. Security Solutions - Constraints

The advanced features of Internet of Things is delivering data and helpful targets to organizations around the world--but it has also introduced new and challenging vulnerabilities [13].

Security alternatives for IoT systems and devices should preferably have the following features

- *Lightweight:* Solutions should reduce the number of calculations and interaction needed given restricted power and computational resources of cellular, ad hoc-enabled gadgets.
- *Decentralized:* they must set up security without referrals to central, long term organizations. Instead, security paradigms should impose the collaboration of all reliable pair nodes in the system.
- *Reactive:* MANETS are formed dynamically and the nodes in the Network are either trustworthy or malicious, they may enter or leave at any time without any information. Security issues in this network should respond to changes in system state. They must aim to identify weaknesses and adjustments. So these alternatives should be sensitive.
- *Fault-Tolerant:* As wireless sensor Networks channels are not reliable and they may enter or leave or may compromise at any time without any information or warning so that the security solutions should be designed not to depend on message sequencing.

The above are not the only considerations. Their importance may vary from implementation in applications

XI. Suggestion Scheme in the Devices for Data Storage and Transformation

a) Encryption to protect data

Securing these sensitive data with trust is the main area to be identifiable or proprietary. This means protection on the IoT device itself[14], when the data is being transmitted to intermediate points, such as IoT gateways, and when it is moving route to final destinations, such as the cloud or a data center for storage and analysis.

This requires not only process steps to identify the specific data to be encrypted, but also a key management scheme to distribute and manage the keys that are used to encrypt the data. Secure storage and access control for keys requires planning — they must be available to permitted people/entities to enable data access, but also properly segregated from the data and stored securely. It might be easy in outlook, but IoT scale and speed is dynamic. The life of Keys based on their length and the algorithm being used, and therefore must be rotated at regular intervals. Losing a key used

to encrypt data in the sense losing the data indirectly. Key management is most crucial functionality in IoT deployments with sensitive data[1,15].

In day to day communication process and data storage confidentiality is maintained by encryption. In recent network environments it is compulsory to adapt some functionality, such as delegation of computations and comparisons of data to untrusted nodes or organizations for further processing. Then the only way is to provide data in encrypted format for further process, Rivest et al suggested in 1978 a remedy for this problem through homomorphic security [14], where operations are performed on encrypted data to maintain confidentiality. Homomorphic encryption techniques allow particular kinds of operations to be performed on the ciphertext as if the operations are conducted on the plaintext [19].

The security requirements for data and methods have become very stringent in the last few decades. Due to the development of technology, a variety of attacks on electronic gadgets are possible. The issue becomes more complicated when data needs to be handled at insecure locations. That is where homomorphic cryptosystems can be used.

Homomorphic Encryption is a procedure by which complicated computations can be calculated on encrypted data just as on plain text. This scheme exhibits this property for all the arithmetic operations and combinations thereof. For example, additive property means E(x + y) = E(x) + E(y) and multiplicative property means E(x * y) = E(x) * E(y). In mixed multiplicative homomorphism means E(x * y) = E(x) * y. In most situations, this is undesirable because it may help to expose details by splitting the encrypted data [8]. However, this is a desirable property if one wishes to have the sum of a group of encrypted values verified without revealing those encrypted values. In voting protocols, this is used to verify the tally of the ballots without revealing what they are.

b) Homomorphic encryption schemes have the following advantages

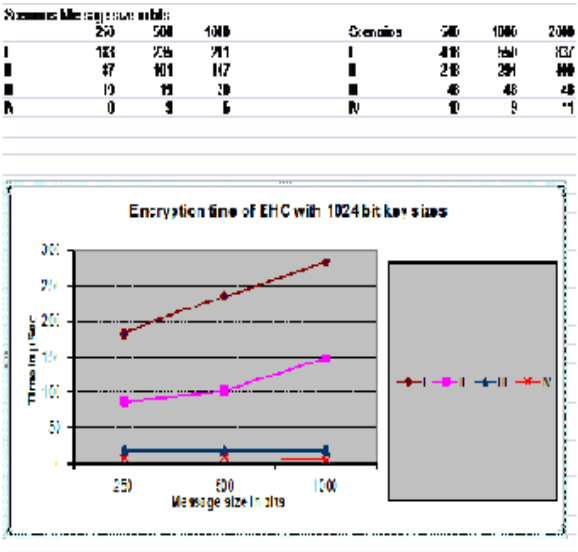
- Cost Saving: As the operations can be performed (addition, subtraction or multiplication) on the cipher text, this saves the encryption and decryption cost at intermediate nodes.
- Secret encryption key and information not revealed: Nodes need not store this encryption key information, as the operation can be performed directly on the encrypted data. The node even if compromised won't reveal the sensitive encryption key and information.
- We proposed a nondeterministic Enhanced Homomorphic Cryptosystem (EHC) for homomorphic Encryption / Decryption with IND-CCA secure theme exhibiting higher performance mainly in processing speed, memory and power consumption16]
- In our scheme we have taken a large prime number ' p ' , another prime number ' q ' such that q < p are taken and a random number ' r ' is taken to make the process nondeterministic. Let the set of plain text information Zp and the set of cipher text functions {+ , - ,* , / and mixed} composed respectively, of the addition, subtraction, multiplication and mixed multiplication modulo m, with m = pq. Let the cipher text be Zc. The security key k = (p, q, m, r) and E(X)=)(mod m). Decryption will be done with the secret key ' p', X=D (Y) = Y mod p. It can be broken if 'p' can be discovered which is not easy to solve.
- Let us see the operations of EHC scheme:-

Key Generation Secretkeygen()
Chose large prime number ' p ' and another prime number ' q '   Calculate m = p * q   Generate a random number ' r '.   R,q and m Kept secret. Secret values r,q and m   Shared key : p
Encryption Encrypt(X,m,p,q,r)   Assume X € Zp   Compute)(mod m) Output Y € Zc
Decryption Decrypt(Y,p)   input Y € Zc   compute X = Y mod p output X € Zp

Fig. 1: Algorithm of EHC

- We constructed proposed new Enhanced Homomorphic Cryptosystem (EHC) with IND-CCA security with better performance than existing schemes mainly in computation, memory requirement and power consumption. Proposed scheme is non deterministic and satisfies additive, multiplicative, mixed additive and mixed multiplicative homomorphism.
- The EHC is additively, multiplicatively, and mixed-multiplicatively homomorphic. Also, our EHC encrypts same plaintext message, 'x', into different ciphertext messages. Thus, even though E1 (x) ≠ E2 (x),but D(E1 (x)) = D(E2 (x)).

We have tested our scheme with four scenarios' with varying the IoT devices and the data size in simulated environment with critical, average, worst and best scenarios'. The results are given below.



XII. How to Protect IOT Systems and Devices

IoT security features vary depending on specific IoT application and place in the IoT ecosystem. So that IoT companies from product makers to semiconductor manufactures should concentrate on building security from the beginning, making hardware tamper proof, planning secure hardware, ensuring secure upgrades, providing standard updates or patches and performing dynamic testing. Developer's focus should be on secure software development and secure integration. Deploying IoT systems, hardware security and authentication are critical measures. For example operators, keeping systems secure with new version, protecting from malware, auditing, protecting infrastructure are the key features.

Major IoT Security Issues we Need to Handle:

Identity and access management
Data integrity
Privacy and confidentiality
Automation and management tools
Data Encryption
Data Authentication
IoT Hardware Issues
Hardware testing is inevitable
Managing updates
IoT security tools and legislation

XIII. The future of Iot

As per recent survey, 86% of respondents said that they were unable to identify all of the devices connected to their networks. 59% were nervous about their device security, and 61% were concerned about integration. More organizations will proceed with IoT implementations in 2025. The surprising thing depends on interoperability among the vendors. This all will be achieved by single plan management only.

In recent industry applications, there will be serious progress toward the integration of AI, machine learning, and deep learning. AI will deliver preliminary business insights from analyzed data with a baseline of algorithms. As computers and other mechanized appliances observe anomalies that conflict with preliminary assumptions, then they refine their knowledge bases by appling machine learning. If the results yielded continue to be incomplete, they will apply a deeper set of algorithms known as deep learning to operate on the data. The goal is precision results of AI at all levels by implementing AI and learning technologies to work together for best results.

XIV. Conclusion

It is recommended to apply the homomorphic encryption scheme in IoT devices and the systems based on the demand when operations required in between transmission.

IoT devices demand more security in handling and processing the data securily. This can be achieved by our scheme very efficiently as the security features meeting the demand of the IoT devices.

References Références Referencias

1. A. D. Wood and J. A. Stankovic: Denial of Service in Sensor Networks, Computer, Vol. 35, No. 10, Oct. 2002; DOI: 10.1109/MC.2002.1039518
2. B. B. Zarpelão, R. S. Miani, C. T. Kawakani and S. C. de Alvarenga: A Survey of Intrusion Detection in Internet of Things.
3. Journal of Network and Computer Applications, Vol. 84, Apr. 2017; https://doi.org/10.1016/j.jnca.2017.02.009
4. M. A. Ferrag, L. A. Maglaras, H. Janicke and J. Jiang: "Authentication Protocols for Internet of Things: A Comprehensive Survey" arXiv, Dec. 2016
5. T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar and Klaus Wehrle: Security Challenges in the IP-based Internet of Things, Wireless Personal Communications, Vol. 61(3), Dec. 2011; DOI: 10.1007/s11277-011-0385-5
6. Article Current research on Internet of Things (IoT) security: A survey
7. Akbar Abbasi "Desirable Security for WSN",International Journal of Computer and Electrical Engineering, Vol.1, No.3, august,2009, 1793-8163.
8. A. J. Menezes, D. B. Johnson, "EC-DSA: An Enhanced DSA", Invited Talks – 7th Usenix Sec., Symp., Jan., 1998, pp. 33-43.Certicom Corp., "Certicom ECC Tutorials".
9. A silverberg "homomorphic encryption plan for cloud services", 2013.

10. Alessandro Sorniotti, Laurent Gomez, Konrad Wrona and Lorenzo Odorico “Secure and Trusted in-network Data Processing in Wireless Sensor Networks: a Survey” Journal of Information Assurance and Security 2 (2007) 189 – 199.
11. Bart Goethals, Sven Laur, Helger Lipmaa, and Taneli Mielik¨ainen, “On Private Scalar Product Computation for Privacy -Preserving Data Mining” Helsinki University of Technology, Finland.2011.
12. Brett Hemenawy and Rafail Ostrovsky, University of Michigan “On Homomorphic Encryption and Chosen-Cipher text Security” in the Proceedings of PKc 2012.
13. Bruce schneier,”Applied cryptography – Protocols ,Algorithms, and Source Code in C” Second Edition. 2011.
14. C. Fontaine, F. Galand, “A survey of homomorphic encryption for no nspecialists” EURASIP Journal on Information Security, p.1-15, January 2007.
15. C. Negus, "Linux Bible: Boot Up to Fedora, KNOPPIX, Debian, SUSE, Ubuntu, and 7 Other Distributions” 2006..
16. C. Orlandi, A. Piva, andM. Barni, “Research Article Oblivious Neural Network Computing via Homomorphic Encryption” Hindawi Publishing Corporation EURASIP Journal on Information Security Volume 2007, Article ID 37343, 11 Pages doi:10.1155/2007/37343.
17. C. Shannon, “Communication theory of secrecy systems,” Bell System Technical Journal, vol. 28, pp. 656–715, 1949.
18. Carlos de marais cordeiro,Dharma praksh Agarwal “Ad Hoc & Sensor Networks” Theory and Applications - Worlds Scoentific.publications-2012.
19. Certicom Corp., "Remarks on the Security of the ECC systems", ECC White Papers, uly 2000.
20. Cherita Corbett, Raheem Beyah, Janise McNair “Computer and Network Security Volume 3 Security in Ad Hoc and Sensor Networks”.-2011.
21. D. Integrity, P. Sakarindr, and N. Ansari, "Security Services IN Group Communications OVER Wireless
22. Infrastructure, Mobile Ad Hoc, AND Wireless Sensor Networks" IEEE Wireless Communications, pp. 9, 2007.
23. D. Micciancio and O. Regev. “Post-Quantum Cryptography, chapter Lattice-based Cryptography”. Springer, 2008