Security Enhancement in IoT Based Systems Through A Collaborative Method Comprising Simplified Encryption Technique

S.Rajarajesware[1]
(Research Scholar,Manonmaniam Sundaranar University,Tirunelveli,TN,Indi a.
email: sivrajarajesware@gmail.com)
Dr.H.Abdul Rauf [2]
(Professor & Dean, Sree Sastha Institute of Engineering and Technology, Chennai, TN, India.
email: harauf@yahoo.com)
Dr.S.P.Victor [3]
(Dean of Science and Associate Professor,St.Xavier's College,Palayamkottai,TN ,India.
email: drspvictor@gmail.com)

ABSTRACT: Internet of Things is a network of things through Internet for the benefit of people. The things that become part of IoT work smarter and ease the works of human. Their automated operations will be very much appreciable if they work as per the predefined and expected procedures for which they are intended. But in case any adversary injects false data, the operations become unreliable and will result in unexpected and in some cases dangerous outcome. To overcome this, in this paper a solution is proposed which will identify such threats and ensure the operations of the system within safe limits.

Keywords—Internet of Things, security, confidentiality, threats

1. Introduction

Internet of Things (IoT) enables various devices that we use on a daily basis to interact with each other via Internet. This ensures the devices to be smart and send the information to a centralized system, which will then monitor and take actions according to the task given to it. IoT can be used in wide range of domains including healthcare, transportation, entertainment, power grids and smart buildings. With a massive amount of devices connected to the Internet and the huge data associated with it, there remain concerns about the security. By security we mean the degree of resistance to, or protection of the IoT infrastructure and applications [1].

Internet of Things comes with a promise of smart world where intelligent devices form collaboration with each other to exchange information among them as well as gather information from the environment and take appropriate decision. Heer et al define Internet of Things as the interconnection of highly heterogeneous networked entities which include various kinds of communication such as Human to Human (H2H), Human to Thing (H2T), Thing to Thing (T2T) and Things to Things. Internet of Things generally consist of five components such as (1) sensors to collect and transmit data, (2) Actuator to trigger a device for particular function, (3) Computing node to process information sent by the sensor, (4) Receiver to receive message from other devices or computing nodes and (5)Communicator to pass messages from one component to another[2].

The most challenging topics in such an interconnected system of miniaturized "things" are security and privacy aspects. Before the IoT existence, corrupted digital systems were mostly unable to act in the physical world. This will change dramatically and dangerously now that corrupted digital systems can operate in and influence the physical world. Authentication and access control technologies are known as the central elements to address the security and privacy problems in computer networks. They can prevent unauthorized users from gaining access to resources, prevent legitimate users from accessing resources in an unauthorized manner, and enable legitimate users to access resources in an authorized manner[3].

Considering a smart car which automatically operates based on the inputs it senses, its operations will be appreciable if it operates in a secured manner. Once its input data are altered by false injections by an adversary, the operations of the car may be uncontrollable and poses danger to the life of the persons who travel in it and also to the outside people who are on their way using the same passage or road. To prevent such kind of undesirable situations, the root cause, that is breach of security has to be addressed. In this paper, it is proposed to find a solution which will prevent these kinds of untoward situations and maintain the perfection that is aimed with such IoT enabled devices.

2. Literature Survey

Abie H et al. [2009] present an adaptive and evolving security (AES), and an adaptive trust management (ATM) approach to autonomic messaging middleware systems, an approach that learns, anticipates, evolves and adapts to a changing environment at run-time in the face of changing threats.
Tao and Peiran [2010] discussed the mechanism for PPPM (preference-based privacy protection mechanism) for IOT, which gives user the right to define the preference of the privacy and helps the SP to realize it so that to protect the privacy information better.
Li You-guo et al. [2011] propose the theory that through the use of middleware, the reinforcement of the system security of the Internet of things can be achieved.
A. Sardana et al. [2012] discussed the requirement of identity management and then presented a framework for identity management for Cloud based Internet of Things. The framework follows a Publisher–Subscriber approach for proper functioning of Internet of Things.
Lui, Xiao et al. [2012] analysed existing authentication and access control methods, and then focused on the design of a simple and efficient secure key establishment based on ECC (Elliptic Curve Cryptosystem).For the access control policy, they have adopted RBAC-based (Role-Based Access Control) authorization method.
Renu Aggarwal [2012] presented views on light-weight RFID security and specified its weaknesses and presented an improved protocol for it.
Zhihua Li et al. [2013] have discussed the major security risks, especially the security problems at the perception layer in the IoT.
Sathish Alampalayam Kumar et al. [2016] have articulated that as more and more IoT based devices get connected to the Internet, it results in the extension of the surface area for external attacks. They have classified those attacks based on the layers that make up IoT and discussed several such attacks with examples. They have also summarized the limitations of the existing security methods.

3. Objective

The main objective of this paper is to identify and incorporate a method which will ensure that the reliability of the IoT device's data and also its authenticity which will be up to the users expectations, even if there are threats like false data injection or adulteration of data generated by the sensors by an adversary. Our method should identify such an erroneous situation which in turn can be used for alerting and to take necessary action to get rid of it.

4. Proposed Work

Our proposed work makes use of a table containing reference values which are permissible for each parameter that the IoT system will use. Each data generated by the sensors will be compared with the table and checked if it lies within the permissible limits. Then to this data generated by the sensor, a simplified encryption process is applied and then uploaded. While retrieving back, the decryption process is applied to get back the original data and the authenticity of the data is ensured by forming and comparing security bytes.

5. Design and Implementation

Our proposed method is explained as follows:

Step 1: For each data generated by the sensor, first it is ensured that it lies within a predefined valid range, by comparing it with a table containing reference values.
Step 2: If yes, Let it be F and find the complement value C.
Step 3: Using a key value K, calculate C XOR K => S.
Step 4: Copy LSB of S and place it in an empty bit position starting from b0 of a new byte formation NBS.
Step 5: Find the encoded equivalent of S by comparing with a mapping table M, and send.
Step 6: On repeating steps 1 to 5 for the subsequent 7 bytes and filling the remaining bits of NBS with the bits at position b0 of those subsequent 7 bytes, we will get NBS as the 9^{th} byte and it will be sent.
Step 7: At the receiving end, the first encoded data received will be decoded by mapping with the table M and its equivalent bit combination will be taken, let it be D.
Step 8: LSB of D is copied into an empty bit position starting from b0 of a new byte formation NBD.
Step 9: D XOR K => C
Step 10: On complementing , C => F.
Step 11: On repeating steps 7 to 10 for the subsequent 7 bytes and filling the remaining bits of NBD with the bits at position b0 of those subsequent 7 bytes, we will get NBD as the 9^{th} byte.
Step 12: Decoding 9^{th} byte will give us NBS value. Now, Compare NBS with NBD.

If both are same,
then the 8 bytes sent from the sensor are secure, original and unaltered
Else
security breach is identified and has to be indicated.

This is explained using an example as follows:

Step i: Let F be the first data generated by the sensor, representing the parameter speed. Let F =>40_{10}, which on comparing with the table containing domain values is considered as a permissible value.

Step ii: on complementing F, we get 255-40. => 215_{10} =>C.

Step iii: Let the key value be 137_{10} =>K.
C XOR K => S => 215 XOR 137 =94

Step iv: LSB of S is copied into bit position b0 of a new byte NBS. For eg:

							0

Step v: S will be compared with a mapping table M and its equivalent code will be taken as its encoded data and sent.

Step vi: The above steps are repeated for n data. For example 8 data, in case sensor generates 8 bit data. For each subsequent data also bit at b0 position will be taken to occupy bit positions b1, b2…b7 respectively of NBS. Hence after every 8 bytes of sensor generated data, the 9th byte becomes the completed byte NBS, which will also be sent.

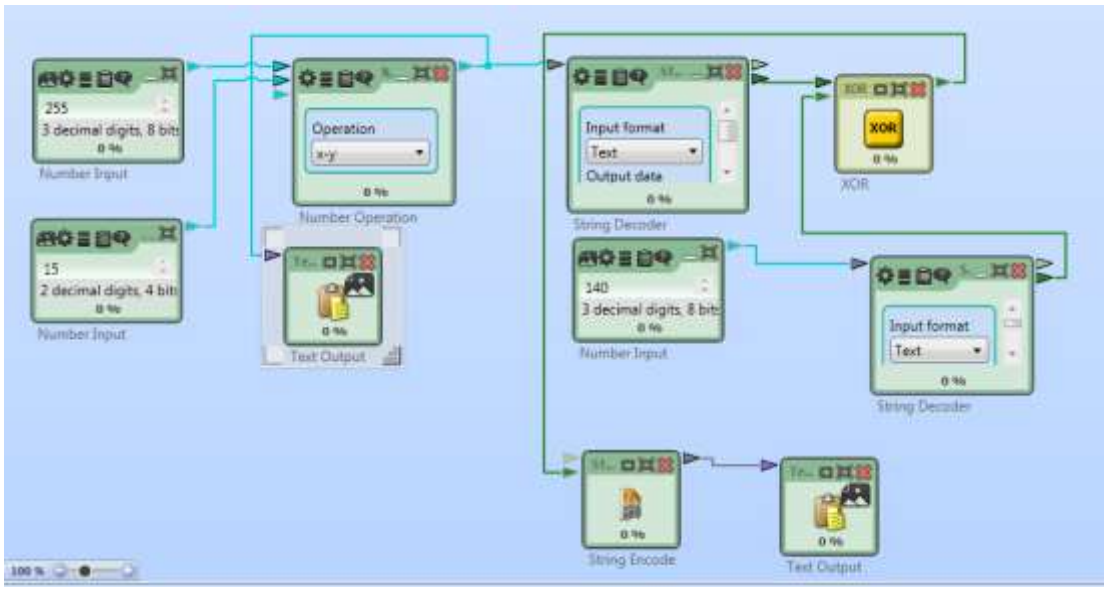
Step vii to xi: At the receiving end, the reverse process of the above steps will be done and a new security byte NBD will be formed.

Step xii: The bytes NBD and NBS will be compared and if both are same then the security of the received set of 8 data is ensured, else a security breach is identified and alarmed.

6. Experimentation and Results

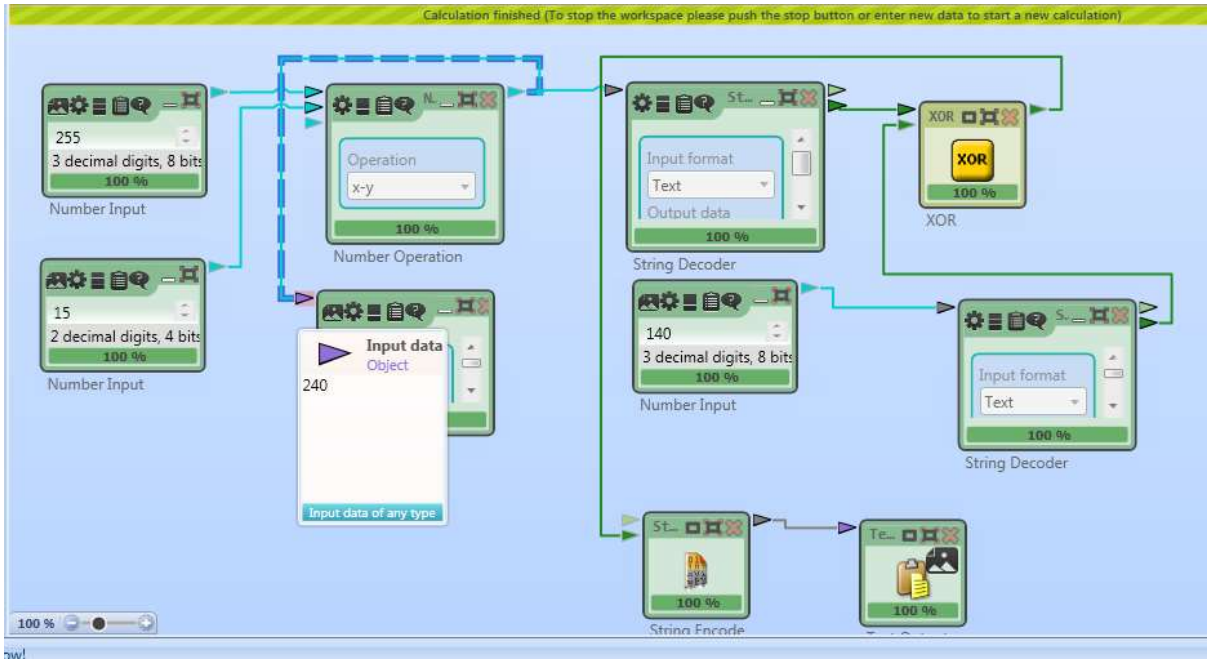
The above technique is experimented and its result samples from the part of sending side are given as shown below.

Before execution:



As an example, here the first data generated by the sensor is taken as F=15.
Complement of 15 is obtained as C=255-15=240.
This is shown below.

After Execution:



Key value to be XORed is taken as K=140. Then the complement value is XORed with the key value. The resulting value is mapped with the mapping table M and its equivalent code will be identified and sent as the encoded data

A portion of the mapping table M is shown below:

Value	Coded Form
033	!
034	"
035	#
036	$
037	%
038	&
039	'
040	(
041	)
042	*
043	+
044	,
045	-
046	.
047	/
048	0
049	1
050	2
051	3
052	4
053	5
054	6
055	7
056	8
057	9
058	:
059	;

The time details for the execution of above steps are as given below:

NR	LOGLEVEL	TIME	PLUGIN	TITLE	
1	Info	10:36:28:023	Workspace	-	Execute model now!
2	Info	10:36:28:046	Workspace	-	Stopping execution.
3	Info	10:36:28:046	Workspace	-	Start stopping ExecutionEngine
4	Info	10:36:28:052	Workspace	-	ExecutionEngine successfully stopped

The table below shows the various parametric values generated by different sensors along with the time taken to upload them without encryption and with encryption. Since, in this example, a simplified encryption methodology together with a technique to ensure the confidentiality of the data is used, these results show very little difference which is almost same for both the processes of uploading data with and without encryption. This implies that our new methodology does not impose any additional overhead in the processing time, which is a very much desirable aspect.

S. No	Speed (kmph)	Fuel (ltr)	Temperature (degree)	Degree of visibility (front cam)	Range of vision coverage (km)	Upload time without Encryption in ms	Upload time with Encryption in ms
1	40	2	28	90	.07	0.170	0.193
2	40	1.95	30	90	.05	0.180	0.201
3	50	1.9	29	90	.04	0.165	0.185
4	63	1.8	31	90	.05	0.213	0.234
5	70	1.73	29	90	.06	0.205	0.227
6	80	1.6	28	90	.04	0.191	0.213
7	82	1.53	28	90	.06	0.187	0.210
8	30	1.41	28	90	.08	0.162	0.185
9	28	1.29	30	90	.12	0.156	0.178
10	50	1.18	29	90	.05	0.177	0.199

Table 1: Data generated by IoT based smart car, with time taken for uploading data without encryption and with encryption.

S.NO	PARAMETER	Min Value	Max Value
1.	SPEED (kmph)	0	150
2.	FUEL (ltr)	.1	5
3.	TEMPERATURE (Degree)	-5	50
4.	DEGREE OF VISIBILITY (FRONT CAM)	0	180
5.	RANGE OF VISION COVERAGE(km)	0	.5

Table 2: Reference values

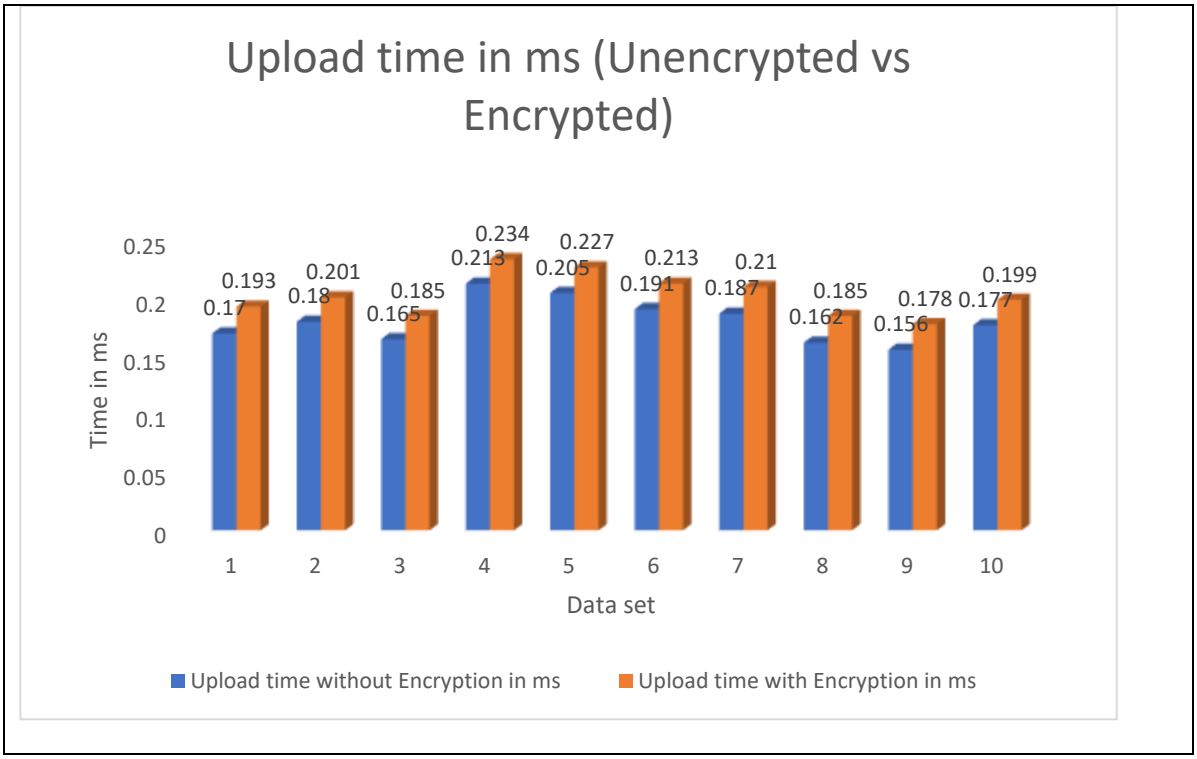


Fig 1: Comparison of upload time for unencrypted and encrypted data

7. Conclusion

In this paper, the possibilities of security violations in an IoT based smart car are analysed, and a collaborative method is devised which includes simplified data encryption and a method to ensure the genuinity of the data by means of secret data formation and comparison. This provides the capabilities of ensuring that the data generated by the sensor are original and not tampered or altered by anyone and ascertains the security of the IoT based device's operation. Also the comparison of each of the data generated against the permissible range provides a mechanism to identify if the sensor is working fine or else if it needs attention by the user. These additional security measures will provide better security in an unmanned automated environment against intrusions.

8. Future work

Further researches in this direction will provide a more secured environment by addressing unnoticed and unexpected threats if any. As a future work, data can be analysed and based on the analysis, forthcoming unexpected or critical situations can be sensed in advance and accordingly prior intimations can be given to the user to get ready to tackle them. This will fortify the security of the overall IoT system's operations.

9. References

[1] Security in Internet of Things: Challenges, Solutions and Future Directions, Sathish Alampalayam Kumar, Tyler Vealey, Harshit Srivastava, 2016 49th Hawaii International Conference on System Sciences, IEEE.
[2] A. Sardana and S. Horrow, "Identity management framework for cloud based internet of things", Proceedings of the First International Conference on Security of Internet of Things, pp. 200-203, 2012.
[3] Lui, Xiao, Chen. "Authentication and Access Control in the Internet of things" 32nd International Conference onDistributed Computing Systems Workshops (ICDCSW), pp.588 – 592, 2012
[4] Zhihua Li et al., "Research on PKI-like Protocol for the Internet of Things", Fifth International Conference onMeasuring Technology and Mechatronics Automation(ICMTMA), pp. 915 – 918, 2013.
[5] Renu Aggarwal. "RFID Security in the Context of "Internet of Things", Proceedings of the First International Conference on Security of Internet of Things, pp. 51-56, 2012
[6] Tao and Peiran, "Preference-based Privacy Protection Mechanism for the Internet of Things", InternationalSymposium on Information Science and Engineering (ISISE), pp. 531 - 534 2010.
[7] Li You-guo, Jiang Ming-fu. "The Reinforcement of Communication Security of the Internet of Things in the Field of Intelligent Home Through the Use Of Middleware", Fourth International Symposium on Knowledge Acquisition and Modeling (KAM), pp. 254 - 257 2011
[8] Abie H., and Balasingham I., "Adaptive security and trustmanagement for autonomic message-orientedmiddleware", IEEE 6th Int. Conference on Mobile Ad hocand Sensor Systems (MASS'09), pp. 810-817, 2009.