Journal of Innovative Engineering and Research (JIER)
Vol.- 2,Issue - 2, October 2019, pp. 16-21 (6 pages)

Security Enhancement of Networked Building Automation System in Airports

NIKHIL RATHORE, SANTOSH PAWAR
Department of Electronics and Communication Engineering, Dr. A. P. J. Abdul Kalam University, Indore
Corresponding Author Email: nikhil.rathore909@gmail.com

Abstract—Automation Systems InAirports (ASIA) are growing very fast, so the needs to protect such applications are increased. The hacking is the greatest problem affected on Automation System (AS) networks. Encryption algorithms play a main role to prevent hacker attacks. On the opposite side, those calculations devour a lot of registering assets, for example, CPU time, memory, and battery power. The principle object of this paper is to join between encryption calculations and hash calculations to get high security in AS. Right now near between the most widely recognized encryption calculations. An examination has been directed for those encryption calculations at various settings for every calculation, for example, square size, Key Length, Cryptanalysis obstruction and etc.In request to acquire the best encryption calculation appropriate for mechanization frameworks to utilize it with the quickest calculation MD5. Show utilized systems in BASIA LonTalk, KNX/EIB and Backnet. Security Enhancement of networked BASIA using the combination of encryption algorithms and hash algorithms. Finally make comparison between LonWorks, KNX/EIB, Backnet and the proposal solution, the experimental result show that the proposal solution and guarantees security demands.

I. INTRODUCTION

Building Automation Systems (BAS) a system that centralizes and integrated monitoring, control, operation and management of mechanical and electrical systems in buildings- In general, integration among all kinds of systems typically found there. The center application region is the programmed control of customary structure subsystems like lighting, HVAC (Heating, Ventilation, and Air Conditioning). Administrations from the security area (e.g., Access control frameworks, Surveillance frameworks, Intrusion recognition frameworks and Fire Detection and alert frameworks) are frequently given by application-explicit subsystems.

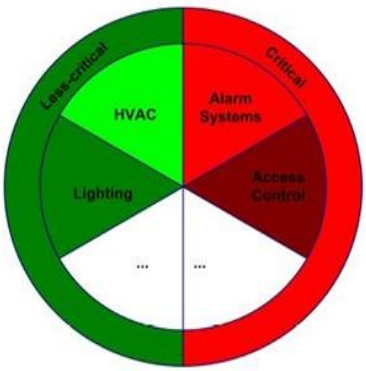

Figure 1: Different types of systems [1]

BAS guarantees the operational exhibition of the office, spare time and cost just as the solace and security of structures staff, to satisfy these requests a specialized framework is fundamental. [1]Communication networks in BAS are typically implemented following a two-tiered hierarchical model. The control level consists of intelligent sensors and actuators interacting with the

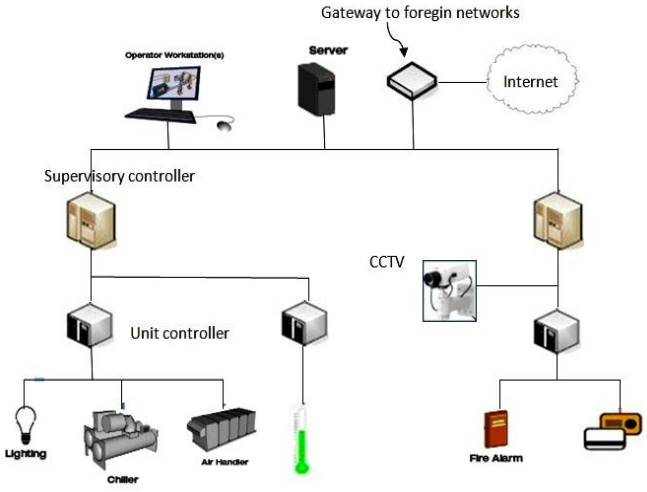

Figure 2: BAS levels functional hierarchy [2]

II. SECURITY REQUIREMENTS

There is common way to provide protection to BAS is to make installations rely on physical isolation and \Security by Obscurity, disengaging the control framework arrange which associates gadgets in the framework and fills in as a way for data move between them from different less secure open systems including the Internet. This confinement, regularly called an air hole, gives the insurance by constraining access to the control organize. Just approved administrators with physical access to the framework approach the control framework organize. Along these lines, it requires human administrators to introduce at the physical area and physically deal with the control framework making the undertaking badly designed and wasteful. This is obviously unacceptable within modern BAS since preventing physical access to the network by isolation is not always possible (e.g., WLANs, public buildings). Moreover, \Security by Obscurity" is a technique that (if at all) provides only temporary protection.

A.To achieve secure BAS, we must do some steps

First, the communication users in BAS that want to securely information interchange (e.g., sensors, actuators, direct digital controllers, management devices) must prove their identities i.e, it must be verified whether the users are what they claim to be (authentication). After that, the information interchange between authenticated users must be protected in a secure manner. This is done by establishing a so called secured channel. A secured channel uses cryptographic techniques to protect information against security attacks while they are transmitted over a network.

B.If we doing these steps we can achieve a secured channel in BAS guarantees the following security demands: [3,4]

- Confidentiality: preventing the message contents leak to the illegitimate users. For this purpose, information should be encrypted with a secret key which only intended receivers have.
- Data freshness: guarantees that the transmitted information is recent and valid at the time of transmission. Replaying of previously sent information can be detected by the users.
- 3-Availability: preventing the denial of the service. Service in the BAS network should be always available to all Users.

C.Secure transmission in BAS.

Secure transmission channel is necessary to protect the transmission of information between users or users and server against malicious interference. This protected channel can be given by cryptographic calculations, utilizing mystery keys. To forestall unintended exposure of these keys, complex key administration is important. The key administration office must give the chance to create and disperse the fundamental keys in a safe way. Moreover, it should likewise be conceivable to disavow old, bargained and shaky keys.

To give extra security, the lifetime of keys will be constrained and controlled utilizing this disavowal system. The key administration system likewise must have the option to deal with highlight multipoint correspondence; in that capacity connections are regularly utilized in BAS.

III. COMPARISON BETWEEN ENCRYPTION ALGORITHMS TO USE THE BETTER IN BAS

Advance Encryption Standard (AES) and Triple DES (TDES or 3DES) are commonly used block ciphers. By design AES is faster in highlight their differences in terms each of 16 rounds. For example, switching bit 30 with 16 is much simpler in hardware than software. DES encrypts data in 64 bit block size and uses effectively a 56 bit key. 56 bit key space amounts to approximately 72 quadrillion possibilities. Even though it seems large but according to today's computing power it is not sufficient and vulnerable to brute force attack. Therefore, DES could not keep up with advancement in technology and it is no longer appropriate for security. Because DES was widely used at that time, the quick solution was to introduce 3DES which is secure enough for most purposes today.3DES is a construction of applying DES three times in sequence. 3DES with three different keys (K1, K2 and K3) has effective key length is 168 bits (The use of three distinct key is recommended of 3DES.).

Hashing Algorithms

Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. [7]

Advantage of hashing key

- Fixed length: in order to a certain algorithm, whatever the size of the data.
- Singularly unique: any cannot produce the same keys for different blocks of data.
- You cannot from the key to access the data at all, but you can find out whether the original data or not by comparing identical keys.

Example of hashing algorithms: MD5, SHA-1, SHA-256, SHA-512

Table1: Comparison between AES, 3DES, DES, RC2, RC6, UR5, UMARAM AND BLOWFISH [3, 4, 5]

Name / Factors	AES	3DES	UR5	RC6	DES	RC2	BLOWFISH	UMARAM
Developed	2000	1978	2011	1998	1977	1987	1993	2010
Key Length	128,198 or 256 bit	(K1.K2 and K3) 168 bits and (K1 and K2 is same) 112 bits	64-bits	128,192 or 256 bits	56 bits	8-128 bits, in steps of 8 bits; default 64 bits	32-448 bits	512-bits
Cipher type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Symmetric algorithm	Symmetric block cipher	Symmetric algorithm	Symmetric cipher algorithm	Symmetric block cipher
Block size	128,198 or 256 bit	64 bits	64 bits	128 bits	64 bits	64 bits	64 bits	512 bits
Key(s)	Single	Single(later divided in 3 parts)	Single	Public	Single	public	public	Single
Cryptanalysis resistance	Strong against: differential, truncated differential, linear, interpolation and square attacks	Vulnerable to differential, brute force attacker could be analyzing plaint text using differential cryptanalysis.	Strong against: differential, truncated differential and linear attacks	Vulnerable to differential , brute force attacker	Vulnerable to differential and liner cryptanalysis ; weak substitution tables	Vulnerable to differential , brute force attacker	Vulnerable to differential , brute force attacker	Strong against: differential, truncated differential, linear, interpolation and square attacks
Time require to check all possible keys at 50 billion keys per second	For a 128 bit key:5×10^{21} Years	For a 112 bit key:800 days	For a 64-bit key:11 years	For a 192 bit key:10^{40} years	For a 56 bit key:400 days	For a 64-bit key:11 years	For a 448 bit key:10^{116} years	∞

Table2: Comparison between hashing algorithms [7]

Name / Factors	MD5	SHA-1	SHA-256	SHA-384	SHA-512
Key length	**128 bit**	**160 bit**	**256 bit**	**384 bit**	**512 bit**
Message size	**$< 2^{64}$ bit**	**$< 2^{64}$bit**	**$< 2^{64}$bit**	**$<2^{128}$ bit**	**$< 2^{128}$ bit**
Block size	**512 bit**	**512 bit**	**512 bit**	**1024 bit**	**1024 bit**
Word size	**32 bit**	**32 bit**	**32 bit**	**64 bit**	**64 bit**
Number of steps	**64**	**80**	**64**	**80**	**80**

 # MD5 is the faster while SHA-512 is the stronger

IV. DEMONSTRATE USED TECHNIQUES IN BASIA

In this section we analyze the security aspects of the two popular BAS: LonWorks/LonTalk, KNX/EIB and BACnet .[8, 9, 10]

1- LonWorks

The communication protocol of LonWorks (called LonTalk) provides a rudimentary security concept based on a four step challenge-response protocol.
LonTalk gives confirmation utilizing a four stage challenge-reaction system. A sender which wants to verify a transmission declares the confirmation bit of its message. Recipients answer with a 64 piece arbitrary number. The sender restores a 64 piece hash esteem determined over the substance of the message and the irregular number utilizing a mutual key. The recipient plays out a similar figuring and analyzes the outcomes

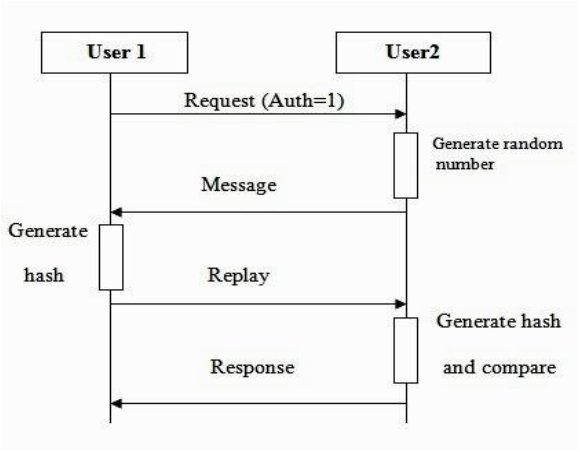

Figure 3: LonTalk security mechanisms

These security flaws in LonTalk:[8,9]

- The authentication services only support the verification of the sender's identity. The identity of the receiver cannot be checked.
- It is not possible to establish communication sessions. Thus, it is always necessary to transmit four messages for authentication, even if a sender transmits multiple data messages to the same receiver.
- The authentication protocol is vulnerable to Denial of Service (DoS) attacks. To start a flooding attack, the attacker sends a lot of messages with the authentication bit set. For each message, the receiver will generate a random number and calculate the necessary hash value. This is time-consuming.

2- KNX/EIB

KNX/EIB doesn't offer instruments to ensure information secrecy, information uprightness or information freshness. Neither does it bolster a devoted validation administration. It just gives an essential access control plot dependent on clear content passwords. Up to 255 distinctive access levels can be characterized, every one of them related with an alternate (in any case undefined) arrangement of benefits. For every one of these entrance levels, a 4 byte secret phrase (key) can be indicated. This plan is accessible for the board correspondence. Since this entrance insurance is simple, KNX/EIB doesn't give the fundamental components to ensure a protected domain.

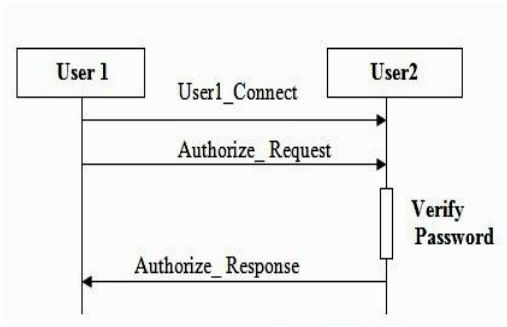

Figure 4: Access control mechanism of KNX

These security flaws in KNX/EIB: [9, 10]

- KNX/EIB does not support mechanisms to manage, distribute keys in a secure manner. Therefore, the keys must be uploaded to the device manually. It is up to the system administrator to guarantee that this upload is performed in a secure environment.
- KNX/EIB is vulnerable to different security attacks.

3-BACnet [11]

It gives AS a lot of services which achieve some security demands like freshness, integrity, authentication and confidentiality of information. BACnet depend on Data Encryption Standard (DES) and a trusted key server which responsible for key management. It used to establish a secure channel between two users to exchange information. Each device must own an initial secret key.

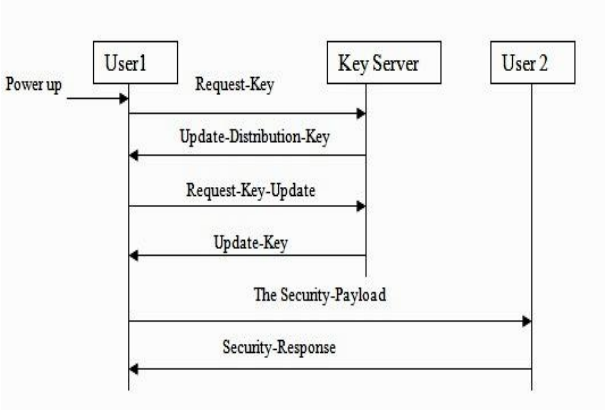

Figure 5: Security services in BACnet

These security flaws in BACnet: [9, 11]

- It used only one encryption algorithm (DES), DES key length 56 bit and weak weak In the face of a lot of attacks.
- The generation and distribution of the initial secret keys is not defined in the BACnet.

Journal of Innovative Engineering and Research (JIER)
Vol.- 2,Issue - 2, October 2019, pp. 16-21 (6 pages)

- The implementation of the key server is not defined by the BACnet.
- Protecting key server against malicious attacks is not found.

V. PROPOSAL SOLUTION OF SECURITY ENHANCEMENT OF BASIA BASED ON HASHING AND ENCRYPTION ALGORITHMS.

- Users mask take permission from administrator to establish connection to automation system network.
- Administrator ensures that name and password is correct after this send accept message to user.
- when user 1 want to connect to user 2, user 1 send to administrator request key message, administrator send to user1 and user 2 start key M1 and update the start key.
- To test transmission channel secure or not secure, user1 send message (S1) to user 2 after encrypt this message (F1= E (M1, S1)) and generate hash of S1
- When the message arrives, User 2 decrypts it, generate hash of S1and compare.
- If ok, user 2 send to user1 message establish connection this mean the channel is secure.

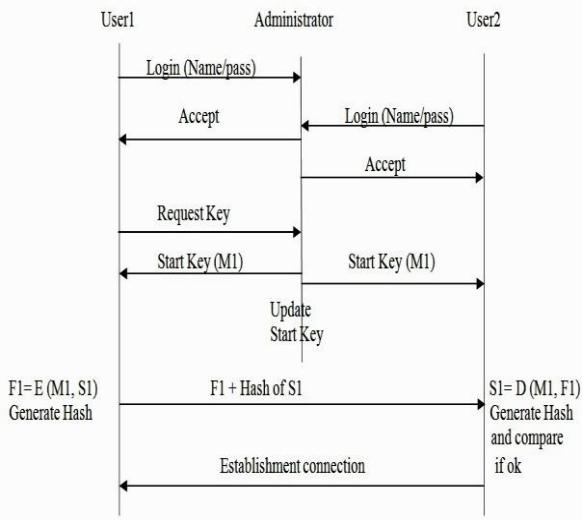

Figure 6: secure channel using hash and encryption

VI. RESULT

	KNX/EIB	LonWorks	BACnet	Proposal
Authentication	32 bit password	64 bit MAC (48 bit key)	DES	AES + Hash
Integrity	-	64 bit MAC (48 bit key)	DES	AES
Confidentiality	-	-	DES	AES
Freshness	-	Random number (64 bit)	Random number (64 bit)	Random number (64 bit)

Table 3: Comparison between LonWorks, KNX/EIB, BACnet and proposal [9, 10, and 11].

The security components of LonWorks and KNX/EIB are not adequate to satisfy the prerequisites on BAS coordinating security subsystems. They can't give a powerful assurance against the security dangers referenced. The security design of BACnet is further developed. Be that as it may, the cryptographic calculation utilized is out of date and ought to be supplanted by a cutting edge one (e.g., Advanced Encryption Standard (AES)). Furthermore, these gauges must be improved to evade certain security defects. A key issue which has not been fathomed by any of these three frameworks is the age and dispersion of the necessary beginning mysteries. Regardless of whether the engineering of the framework itself is secure, an instrument must be accessible to appropriate the underlying insider facts in a safe way.

VII. BAS EXPERIMENTAL PROGRAM

1. Socket programming

A socket is one of the most fundamental technologies of computer networking. Sockets allow applications to communicate using standard mechanisms built into network hardware and operating systems. Although network software may seem to be a relatively new "Web" phenomenon, socket technology actually has been employed for roughly two decades.

2. End-to-end encryption

Continuous protection of the confidentiality and integrity of transmitted information by encrypting it at the origin and decrypting at its destination. For example, a virtual private network (VPN) uses end-to-end encryption.

3. Encryption and decryption in BAS program

a. Hash after Encryption

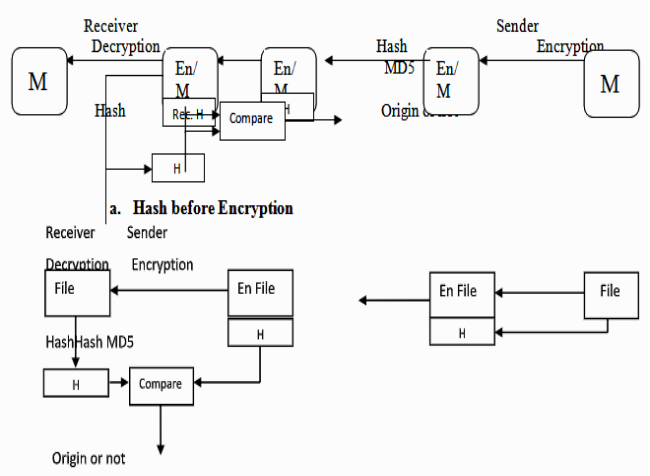

Figure 7: BAS program encryption and decryption block diagram

BAS Message format

Message Type	Message sender	Message content	Message receiver

1- Message Type
EX. “Sign up” - “Login” - “Upload request”
“Upload request” - “Accept”, “Reject”
“Message” - “Cipher message”

2- Message sender: The user who sent the message.

3- Message content: Message body.

4- Message receiver: The user who will receive the message.

VIII. CONCLUSION

The main object of this paper is to combine between encryption algorithms and hash function to obtain high security in automation system. We have compared between the most common algorithms to performance evaluation of these algorithms on encryption speed. AES is faster and more efficient than other encryption algorithms except UR5 and UMARAM. We try to incorporate good features of UMARAM, AES and UR5 in a single algorithm, which can perform well on all latest platforms for all kinds of automation systems. In hashing, MD5 is the faster while SHA-512 is the stronger. We analyze the security aspects of the three popular BAS: LonWorks/LonTalk, KNX/EIB and BACnet and give Proposal to increase security aspects in BAS. Use AES instead of DES. Finally make comparison between LonWorks, KNX/EIB, BACnet and proposal, in order to show that the proposal guarantees security demands.

REFERENCES

1. W. Granzer, Fritz Praus, and W. Kastner, “Security in Building Automation Systems,” in Proc. IEEE Int. Workshop Factory Commun. Syst., 2010, pp. 205–214.
2. Wolfgang Kastner, Georg Neugschwandtner, S teffansoucek, and H. Michael Newman “Communication Systems for Building Automation and Control” Vienna University of Technology, Inst. of Computer Aided Automation, Vienna, Austria, IEEE, VOL. 93, NO. 6, JUNE 2005.
3. J. Douglas Selent, “The advanced encryption standard,” RIVIER ACADEMIC JOURNAL, VOLUME 6, NUMBER 2, FALL 2010.
4. Ramesh G, Umarani. R, ” UR5:A Novel Symmetrical Encryption Algorithm With Fast Flexible and High Security Based On Key Updation”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012 Page 16-22. 2010.
5. G. Ramesh, and R. Umarani “A Comparative Study of Six Most Common Symmetric Encryption Algorithms across Different Platforms" International Journal of Computer Applications (0975 – 8887) Volume 46– No.13, May 2012
6. Harshraj N. Shinde, Aniruddha S. Raut, Shubham R. Vidhale, Rohit V. Sawant, Vijay A. Kotkar“A Review of Various Encryption Techniques”, International Journal Of Engineering And Computer Science ISSN:2319-7242, Volume 3 Issue 9 September, 2014 Page No. 8092-8096.
7. Donald L. Evans, Secretary, Philip J. Bond, Under Secretary and Arden L. Bement, Jr., Director "The Keyed-Hash Message Authentication Code (HMAC)" Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, USA, MD 20899-8900
8. Hee Dong June “Improving the security in interconnecting building automation systems to outside networks" THESIS Submitted in partial fulfillment of the requirements for the degree of Master of Science in Computer Science in the Graduate College of the University of Illinois at Urbana-Champaign, 2011.
9. Wolfgang Granzer and Wolfgang Kastner "Security Analysis of Open Building Automation Systems" Vienna University of Technology, Institute of Computer Aided Automation, Automation Systems Group Treitlstr. 1{3, 1040 Vienna, Austria
10. Fritz Praus, Thomas Flanitzer, Wolfgang Kastner, Secure and Customizable Software Applications in Embedded Networks, Institute of Computer Aided, Automation Systems Group ,Treitlstraße 1-3, A-1040 Vienna, Austria
11. David G. Holmberg, “BACnet Wide Area Network Security Threat Assessment" U.S DEPARTMENT OF COMMERCE National Institute of Standard and Technology, Building Environment Division, Building and Fire Research Laboratory Gaithersburg, MD 20899-8631.