ISSN:0975-9646

Assuring Data Integrity through a Novel Message Authentication Code with Iterative SHA-1 and Secret Key Randomizer

Megha Sunhare, Prof. Mahendra K. Verma
Department of Computer Science & Engineering
Sushila Devi Bansal College of Technology, Indore (M.P) -453331, India

***Abstract*— Network security deals with effective handling of vulnerable situations of information exchanges to prevent performance degradations. Now, the recent communities and internet users are working to design highly protected zones for sensitive information transmissions with minimum delays. It will somewhere reduce the attack space for malicious users. Thus some additional security mechanism needs to be embedded along with existing transmission channels. Mainly the intensions are to for serving better defence against the integrity attackers. Previously, the message authentication codes are working in this arena to get intense security against the various vulnerabilities. This work presents a novel iterative message authentication code with adapted key size, compression codes and randomiser function to get robust security, high performance and reduced resource consumptions. The above functions are high collision resistant and offer larger privacy degrees. At the analytical level of evaluation the approach is satisfying all the parametric means of research goals.**

Keywords—Network Security, Integrity Controls, Message Authentication Codes, Collision Resistance, Adaptive Key Size, Compression Code, Randomizer;

I. INTRODUCTION

In today's world communication and their means requires reliability between the exchanging parties and desire trustworthy computation. Thus, the system is required with robust security mechanism and strong cryptographic constraints to prevent the attacks resistant mechanism. Each participating entity requires higher privacy of transmitted data and demands better confidentiality against the threats and attackers. As far as the current situations are considered the secret information exchanges suffers from various kinds of vulnerabilities and errors occurring in transmissions. Their intension is to make the data protected under some open communication channels. Thus, to guarantee the better security some additional security primitives must be added with formal approaches of authentications. The two major pillars of security is confidentiality and authenticity which is a matter of individual requirements or nature of transmissions for building safe communication between the parties. In open network or internet the user demands for high speed and packet base data delivery which somewhere lacks with the security rules and creates the attack prone surface. Data confidentiality is provided using cryptosystems and the integrity and access control is served by authentication mechanisms. Latest efforts in cryptography are aimed at designing new, secure, symmetric schemes that achieve the security goals of confidentiality and authenticity simultaneously. Commonly they are known as authentication & encryption (AE Approaches). These hybrid approaches needs to satisfy the massive and robust security demands of users. However the growing demands for many applications and Internet protocols, standardization organizations have claimed their intention for a specification of such schemes, which is lacking till now.

1.1 Understanding Security

High defense against security vulnerabilities or attacks demands complete controls at different working stack of its present infrastructure. Further reducing it might be said that, there are two areas that you need to consider [1]:

- Infrastructure security involves controls (such as firewalls, perimeter security, etc.) relating to the nuts and bolts of the network environment, that will help protect it from external attack. These attacks include infrastructure threats like viruses and worms, but also less lethal ones such as spam. The focus of infrastructure security should be on preventing malicious activities which causes drops in the actual working of the system.
- Service security is even at higher risk associated with it. It involves defending the key system, application, and information from both inappropriate access and illegal use. Identity access management is typically the best approach to protecting these key assets and services that your IT organization provides.

For getting the deeper view of above security primitives first the requirements needs to be understood clearly.

1.2 Why Security Breaches Occurred

Security violations and risk areas are primarily vulnerable to some of its environmental factors which somewhere lack towards lack in protection levels. Some of the factors are [3]:

- Operating System Vulnerabilities
- Poorly Configured Firewalls
- Weak Access Structures & Password
- Loose Authentication
- Weak anti-malware controls
- Lack of Monitoring and Session Management
- Poor patch management
- Lack of automated de-provisioning

But, there are a number of areas of security that are often ignored by various IT organizations, and these can drastically amplify the risk of a booming security violation. These circumstances need unambiguous attention and rectification, and include [4]:

i. **Insufficient User Authentication**—the typical username/password validation methods are grossly poor to defend against security breach, particularly with the creative social engineering attacks that have been used recently. Strong authentication is required, and different methods should be used based on a number of background factors. Hardware tokens have been commonly used, but the recent breach of Secure ID tokens, as well as the cost and effort associated with hardware tokens, make this an unappealing option.

ii. **Insufficient Regular User Access Validation**—As a user goes through role change, promotions, etc., their access privileges are frequently not attuned to reproduce only their present task. Although many companies validate user access rights occasionally, it should be done on a formal and regular basis, and it should preferably be automated so that it can be done quickly and easily. Lack of regular validation can lead to increased risk due to SOD (segregation of duties) violations.

iii. **Lack of System Controls on Privileged Users**—a prime cause of security breaches, privileged users, often have more access than they really need for their job. By definition, these users need broad access rights to do their job, but "broad" shouldn't imply "unlimited." Careless or malicious actions can have devastating effects on your critical assets.

iv. **Lack of Information Use Control**—controlling access to information is not enough protection. You must control use of information also in order to help ensure that it isn't disclosed or stolen. This weakness has been a contributing cause to some of the most visible security breaches of the recent past.

v. **Lack of Continuous User Monitoring**—apparently in the Wiki leaks breach, nobody noticed that someone was copying thousands of sensitive documents from military systems over a short period of time. Many security breaches could be detected with a comprehensive approach to monitoring user activity for suspicious activities. As a result, the lack of effective and continuous monitoring of user activity is also one of the most important contributors to a high risk of security breach.

II. BACKGROUND

Computation involves massive processing along with heterogeneous data support which is quite expensive for the user to purchase permanently, thus along with several other web services now the security is also getting this tradition followed. Some of the basic security concerns of the system are authenticity, fine grained data access, confidentiality, privacy, integrity etc. To ensure the control of client over such system more robust security mechanism is now available with the recent technologies which make data unreadable. The problem associated with the traditional security systems is that they are having lesser control and known policies which gives a vacant space to attacker for planning his malicious activity. Thus here comes the importance of security primitives. During the last few decades security mechanism had changed a lot with users requirements. All they need to satisfy few constraints. Some introductory details are covered here for better understanding of the document.

2.1 Importance of Cryptography

It provides better information security over the systems for user's important data and his privacy constraints. Some of the well known techniques which work collaboratively for achieving the objective are confidentiality, data integrity, and user authentication for both sender as well as receiver. Some of the well known cryptographic goals are:

(i) Data Confidentiality for protecting the user's secret information along with proper privacy concerns.

(ii) Data Integrity offers protection against the unauthorized modification of content during the communication.

(iii) Authentication techniques are used for verifying the identities of users or communicating entities.

(iv) Non-repudiation is a technique which prevents an entity from denying previous commitments or actions.

(v) Data Availability is a technique which provides access to data and techniques in the required manner without delay.

III. RESEARCH MOTIVATION

Enhancing the security of data in a any web server is the growing area of work for researchers. They were concern with prominent authentication encryption (AE) with configurable policies. But to assure this client uses encrypted data to be send to remote storage. Traditional mechanisms are worked many times and extensive studies of them open various ways to beat them. Thus there must be some modification performed which increases the level of security for the users information with reduction in performance drops. These areas of security are getting complex day by day as the number of users gets exponentially increased. These large users are highly concerned with the data losses, unauthorized leakages, robust authentication, malicious users handling, services failures & hijacking of sessions while accessing their information. After studying the various issues related to information security and approaches used to solve them the work identifies some of the problems which remain unaddressed. Few of them are mentioned here as the basis of the proposed work. This work aims to perform comprehensive analysis on the traditional AE approaches and their properties. Moreover, we also make a contribution by suggesting a new message authentication scheme for improving the AE and introduces an extra functionality. The suggested functionality will leads towards effective security with improved performance statics for an open ended system or lightweight system such as mobile devices or its simulations. The approach includes independent confidentiality and authenticity resynchronization designs.

As the work[15] suggested two novel algorithm for applying authentication to short messages on mobile based light handed devices. These application are comes under the category of pervasive computation. It takes the facility by

considering the fact that the authentication must be applied along with the encryption. By embedding the encryption with authentication codes the robustness of the security primitive can be further increased. It also preserves the integrity of secure message exchanges using message authentication codes (MAC) over the public channels. Here the security is applied either computationally or unconditionally secure. The unconditionally secure message authentication code (MAC) is provided having unlimited computational power requirements. But with unconditionally secure process, universal hash function is used which is having limited computational power. The preliminary condition for unconditionally secure message is that the key used here is only valid for defined messages and their sizes. But somewhere the management of these small keys for limited uses is very complex in case of unconditional secure authentication, most of the times the real life application uses computationally secure MAC. Thus the later one can be use for authenticating the variable and arbitrary number of messages using the same key.

Computationally secure MAC is categorized into three major types based on their design:

(i) Block Cipher (CBC-MAC, XOR-MAC, PMAC)
(ii) Cryptographic Hash Function (HMAC, MDx-MAC)
(iii) Universal Hash Function Family (Two Round Pseudorandom Function, UH-MAC)

The universal Hashing based MAC is getting the better performance when compared to block cipher or cryptographic hashing-based MACs. In literature the fastest MACs are based on universal hashing. The main reason behind the performance advantage of universal hashing-based MACs is the fact that processing messages block by block using universal hash functions is orders of magnitude faster than processing the block by block using block ciphers or cryptographic hash functions. Carrying forward the work of improving the message authentication codes it resolves the problems for shorter messages. It preserves the privacy and integrity using an encryption algorithm and authenticating them using standard MAC algorithm. Specifically the shorter messages are emphasized more here. The driving motive behind the investigation is that using a general purpose MAC algorithm to authenticate exchanged messages in such systems might not be the most efficient solution and can lead to waste of resources already available, namely, the security that is provided by the encryption algorithm. The paper effectively uses Negligible Functions, IND-CPA (Indistinguishability under Chosen Plaintext) and secure encryption algorithms. The key idea behind the proposed techniques is to utilize the security that the encryption algorithm can provide to design more efficient authentication mechanisms, as opposed to using standalone authentication primitives. Extensive analysis and evaluations are proving the effectiveness of the given approach.

Message authentication codes are very popular means of digest generation and studied most by the researchers. Its practical implementation includes SSL, TLS, IPSec, Kerberos etc as an access control and authentication protocols. The security of authentication codes for messages lies on the complexity of regeneration of transmitted message by its captured digest and follows one way hash property. Thus to design effective MAC algorithm it should follows following properties along with the given hash algorithm.

(i) It is complex to regenerate the message with digest without knowing its key.
(ii) It is complex to regenerate the messages having similar MAC codes.
(iii) It is complex to regenerate the similar message with different MAC combinations.

VI. RELATED STUDY

During the last few years the message authentication codes and their structure had changed dynamically to satisfy the new requirements of web security. Among them some had applied the previous techniques on new areas and some had modified the way hashing operations executes. Some of them reflects the direction of this work and covered here as surveyed literature.

In the paper [8], NIST has suggested a new authentication standard under its FIP publication. The suggested standard uses HMAC (keyed-hash message authentication code) using cryptographic hash functions. HMAC can be used with any iterative FIPS-approved cryptographic hash function, in combination with a shared secret key. The cryptographic strength of HMAC depends on the properties of the underlying hash function. Further modifications and enhancements with HMAC are performed in [9] also. The suggested schemes of NMAC and HMAC are proven to be secure as long as the underlying hash function has some reasonable cryptographic strength. The paper is also presented with a qualitative and quantitative evaluation to analyze its applicability. The approach uses direct hash function or its compression variants as a dark box API which can be used by massive security providers. It prevents birthday attacks, DoS attacks and many more with its robust construction design. At some of its iterative functions cipher block chaining based hash is used for exhaustive analysis. However, their practical relevance against these functions is negligible given the typical hash lengths like 128 or 160, since these attacks require knowledge of the MAC value. In addition to provide better view of CBC-MAC, the paper also provides a method of building secure PRFs that can be used in a wide range of applications. On the other hand, PRFs are very useful in applications, but one typically needs PRFs on long strings. The CBC Theorem provides a provably-good way of extending the basic PRFs, which work on short inputs, to PRFs that work on longer inputs.

In the paper [11] the attack defense mechanism is developed using the message authentication codes. For achieving their goals the paper also proposed a novel packet passport system to address the challenges. A design of a packet passport system uses an optimized MAC with low message overhead. A packet with a valid passport must have originated from the claimed source. The packet passport system can be incrementally deployed without introducing extra control messages. It also provides incentives for early adoption: a domain that deploys packet passport system can prevent other domains from spoofing

its source identifiers. Preliminary analysis of the work suggests that the packet passport system can be implemented at high-speed routers with today's technologies. Here the packet passport may be implemented as an IP option or as a shim layer. Paper also claims that the design is feasible with today's hardware technology. The paper [12] suggests another variant of MAC named as XOR MAC which includes parallelism, incremental behavior and provide more robust security. The paper had implemented a finite pseudorandom function (PRF) using instantiated DES with yields of CBC MAC. The developed PRF is unbreakable in defined time boundaries which protects the integrity and confidentiality of the past messages. The proof serves the linear algebraic techniques with its XOR implementation with an associated full rank matrix. The analysis shows that XOR schemes are actually more secure than the CBC MAC, in a sense that we can make precise.

In the paper [13], an AKA protocol is suggested with some enhancements by generating the specific keys for sessions of visitors using VLR/SGSN for authentication mobile stations. This protocol is called as E-AKA (Efficient –AKA). It removes the problems affecting the HLR/AuC (home location registers and authentication centre). AKA works for UMTS authentication and key agreements for enhancing the security facilities of third generation mobile network. The approach reduces the network traffic, signaling message between entities. This is achieved by reducing a size n array of authentication vector and the number of messages between MS and HLR/AuC. A security analysis and comparison with related work shows that E-AKA is more efficient and a secure authentication is achieved. For further improving the security of web applications and loaded servers for authentication the paper [14] gives a study on use of elliptic curves cryptography (ECC). It is an alternative approach for achieving the confidentiality and integrity like RSA, DSA and DH. It provides the highest strength-per-bit of any cryptosystem known today with smaller key size resulting in faster computations, lower power assumption and memory. ECC is more secure when small key size is used. It also provides a methodology for obtaining high speed, efficient and scalable implementations of protocols for authentication and key agreement. The present paper consists of ECC based authentication protocol with zero knowledge property.

Some of the papers emphasizes on the speed with high protection for their real time applications with digital contents such as videos, audios, games, stocks etc which was used in content distribution network (CDN). The paper [16] covers the security organization in such networks. The paper provides protection against the delay sensitive systems for malicious access blocking and authentication of users. The system is designed to efficiently process long sequence of bits. The paper also proposes a novel signature amortization technique based on trapdoor hash functions for authenticating each and every individual data blocks in the stream. It works for each and every intermediate blocks in the stream to avoid the transmission loss and provides constant memory requirements for sender and receivers. In the paper [17] a novel method is proposed as Data-Transparent Authentication (DaTA) with reduced communication overhead to validate data streams. It is based on the timing correlation of data packets between the sender and the receiver. Particularly, the inter packet delays are utilized and some selected packet delays are slightly adjusted (in a range). At the evaluation end, proposed system prevents the malicious access to system with ECC approach to provide the senders and receivers privacy.

V. PROBLEM DEFINITION

After the deep survey analysis, we have found some of the problems associated with traditional MAC which needs to be overcome for further improving the approach. Mainly the work emphases over improvement of HMAC with MD5 as its hash function. Apart from that are some other variants of hash available which can also be analysed.

(i) The existing HMAC is weak collision resistant and hence require strong cryptographic controls which sometimes not showing the proper digest generation for shorter length messages. Also the hash values for single blocks are compromised due to this nature.

(ii) Authentication must work in collaboration with encryption algorithms for implementing AE, which might affects the actual performance of authentication and encryption as their originals.

(iii) Flipping of arbitrary bits in a single block will increase the probability of data corruption because here we not knows its initial value throughout the encryption while using CFB mode blocks.

(iv) The performance over memory and speed of HMAC can be further enhanced using another function of similar hash family. This embedded hash will server faster responses for different message types.

VI. PROPOSED WORK

Message authentication codes (MAC) is used to provide data confidentiality and integrity of message communication between the two parties and authenticate their digital content and authority. It is most important entity for providing the security against the various data modification attacks occurring in e-commerce, emails etc. This work introduces a novel message authentication codes with improved performance and will resolve above mentioned issues of traditional approaches. It is having the 320 bit key requirements with a strong encryption algorithm. Existing algorithms uses only 160 bit keyed hash function with SHA or MD algorithms. Performance evaluation will leads towards effective development of practical solution without knowing the internal details. The proposed work uses randomizer function along with the compression codes to assure high collision resistant. It also offers privacy preserving nature. The complete process of proposed MAC is given as:

(i) Initialize the algorithm

(ii) Take the input message from user

(iii) Capture the Users Key Details for Private Key Generation

(iv) Divide the message into M blocks of length 512 bytes and pass the above details to generate the set of 320 bit Key using Randomizer Function
(v) Select one key for each block of message
(vi) Compress the message blocks into Mk Units
(vii) Apply bits padding by inserting the 0 bit in the key at the start to make it up to block size
(viii) Apply prefix and suffix of key and add it to the lsb and msb components of message (256 bits each)
(ix) Apply the SHA-1 algorithm for generating the digest
(x) Add rounds of Iteration
(xi) Perform a circular shift by n bits of hash code and the key with m bits to generate the new hash and key
(xii) Apply XOR or original key and the new hash code to produces new key hash code
(xiii) Apply addition of hash code with shifted key to generate the sash based shifter key
(xiv) Add hash code with transformed shift key block for generating the variable hash code
(xv) Apply XOR of two newly generated key hash combinations for getting the desired message authentication code (MAC)
(xvi) Apply XOR of two generated key shifted hash with hash shifted key to get final m (320) Bit MAC code

Here the security of MAC will depends on the behaviour of hash codes. The length of generated digest depends on the possible combination after which the intruder can affects the integrity constraints. The suffix and prefix are provided with additional hash computation which is more robust and stronger defense against the replay modification, substitution, birthday paradox and denial of service attacks. It bigger key size strong cryptographic primitives made it infeasible to break. As security mechanism will follow the property of confusion and diffusion thus the XOR and shifting operations will serve the goals. The use of pseudorandom function and compression function will achieve the memory and speed requirements of the system

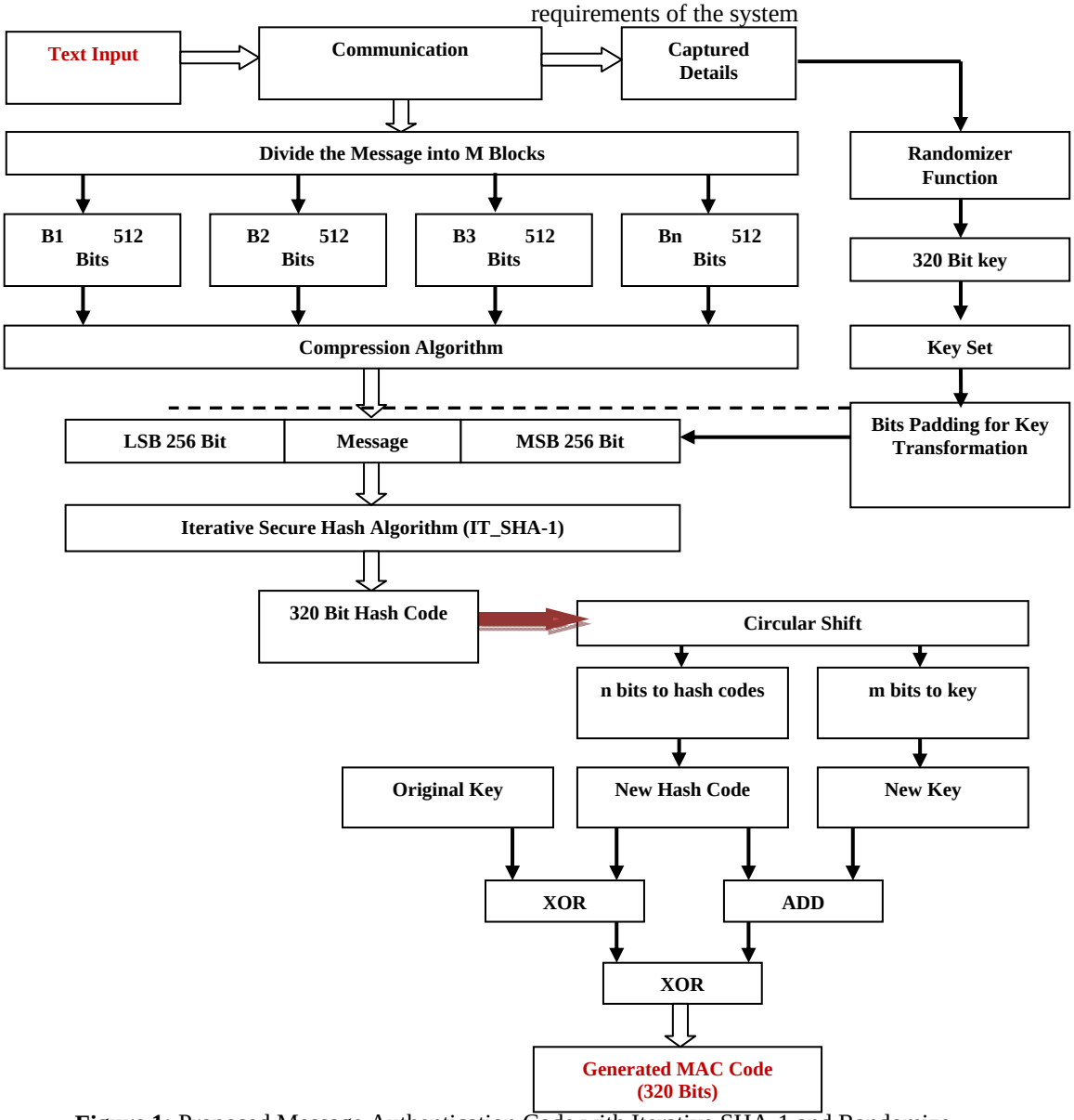

Figure 1: Proposed Message Authentication Code with Iterative SHA-1 and Randomize.

VII. EXPECTED BENEFITS

At the initial level of our research we get the following benefits.

- It provides an efficient way to make sure the message has not been tampered or fabricated over transmission channels.
- It offers a great way to achieve data integrity, authentication and encryption simultaneously in a single shot.
- Data isolation and access control can be guaranteed by using access and key policies for various types of user. Policies are used here to define finer grained access control.
- Dynamic operations on data block are supported like an update, delete and append. This mechanism will improve the efficiency of the system due to parallel processing of data updating and its encryption.
- It retains reliability on hash based digest with collision resistant property and ensures the process of data storage protected against unauthorized access.
- It protect data from different attacks at client end like birthday paradox and repudiation and serve the sole purposes of security with minimal computation cost
- Pseudorandom and compression function along with its higher size (320 bits) will increase the strength of key which ultimately increases the robustness of authentication and encryption.

VII. CONCLUSION

This paper deals with collision resistant problem associated with traditional message authentication codes which gives open space to attacker for violating the integrity validations. Also it causes high computation loads on small end devices and generates the probability of several attacks such as reply, modification DoS etc. After getting the in-depth analysis of problem this paper develops and iterative message authentication code solution with some newly added functionalities to resolve the above problems. Mainly the system works towards improving the HMAC with its performance drops and get the highly secured digest with smaller size. This embedded hash will server faster responses for different message types.

REFERENCES

[1] J. LAWRENCE CARTER AND MARK N. WEGMAN "Universal Classes of Hash Functions "IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598 Received August 8, 1977; revised August 10, 1978

[2] Tor Helleseth "Universal Hash Functions from exponential sums over finite fields and Galois Rings" published in Springer 1996

[3] Victor Shoup"On Fast and Provabaly secure message authentication based on universal hashing" published in Proc. Crypto 1996

[4] Basel Alomair, Andrew Clark and Radha Poovendran"The power of primes: security of authentication based on a universal hash-function family" J. Math. Crypt. 4 (2010)

[5] Basel Alomair and Radha Poovendran"E-MACs: Towards More Secure and More E_cient Constructions of Secure Channels"

[6] Adrian Perrigy, Ran Canetti,z J. D. Tygary Dawn Song" Efficient Authentication and Signing of Multicast Streams over Lossy Channels" IBM 1999

[7] Information technology - Security techniques - Message Authentication Codes (MACs) ISO 1999

[8] FEDERAL INFORMATION PROCESSING STANDARD PUBLICATION The Keyed-Hash Message Authentication Code (HMAC)

[9] Mihir Bellare,Ran Canetti,Hugo Krawczyk "Keying Hash Functions for Message Authentication "An abridged version of this paper appears in Advances in Cryptology Crypto 96 Proceedings.

[10] Mihir Bellare Joe Kiliany Phillip Rogawayz "The Security of the Cipher Block Chaining Message Authentication Code" Journal of Computer and System Sciences, Vol. 61, No. 3, Dec 2000

[11] Xin Liu and Xiaowei Yang, David Wetherall and Thomas Anderson"Efficient and Secure Source Authentication with Packet Passports"

[12] Mihir Bellare⋆ Roch Gu´erin† Phillip Rogaway"XOR MACs: New Methods for Message Authentication Using Finite Pseudorandom Functions"paper appeared in *Advances in Cryptology – Crypto* 95 *Proceedings*

[13] Ja'afer AL-Saraireh"Efficient And Secure Authentication And Key Agreement Protocol"International Journal of UbiComp (IJU), Vol.2, No.2, April 2011

[14] Manoj Kumar "A Secure And Efficient Authentication Protocol Based On Elliptic Curve Diffie-Hellman Algorithm And Zero Knowledge Property "International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-5, November 2013

[15] Basel Alomair, Member, and Radha Poovendran, Senior Member "Efficient Authentication for Mobil and Pervasive Computing"IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 3, MARCH 2014

[16] M.Muthuselvi, P.Jeevananthini"Authentication of Online Digitized Content Using Trapdoor Hash Function Method"International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, March 2014

[17] G.Dhivya,N.R.Jayashree"Message Authentication And Source Privacy Using BAC Technique In Wireless Sensor Networks" The International Journal Of Engineering And Science (IJES) Volume 4 Issue 3 2015