Digital Signature and Blowfish Algorithm Based Multilevel Security Model for Intrusion Detection System

Ritu Makani
Department of Computer Science & Engg.
GJUS&T Hisar (Haryana)

Yogesh Chaba
Department of Computer Science &Engg
GJUS&T Hisar (Haryana)

Abstract: **Spread of network communications have lead to the requirement of the safe and secure environments .Intrusion Detection System (IDS) is a tool used to detect unauthorized access to a network. An IDS usually performs this task in one of the two ways, with either anomaly based detection or signature-based detection. Today's embedded and network systems need system and data security more than ever before. Encryption algorithms play a major role in the information security systems and can be used for several kinds of data security besides providing authentication, the assurance that a message came from whom it says it came from, and also non-repudiation, a way to prove beyond a doubt that a particular sender was the originator of a message. Present paper proposes the framing of a multistage security model using blowfish algorithm in combination with DSA and Hashing techniques like MD5, SHA1 , SHA256, SHA512 to provide a three stage check to ensure data security, pattern matching for preventing evasion of IDS and authentication before decryption to provide system security. Comparison of different hashing techniques is done to compute digital signature components.**

Keywords : IDS, Encryption Algorithm, Blowfish, Cryptography, Hashing Techniques.

I. INTRODUCTION

Networked communications are the need of the day in many facets of life, be it education, business, defence or administrative tasks. But security of these network communications and the data shared is the utmost concern. Security techniques help keep private data private. Secure data transmissions prevent contact lists and personal e-mail from being read by someone other than the intended recipient, keep firmware upgrades out of devices they don't belong to, and verify that the sender of a piece of information is who he says he is. Data security techniques have a reputation for being computationally intensive, mysterious, and fraught with intellectual property concerns. Straightforward public domain techniques that are both robust and lightweight do exist. One such technique, an algorithm called Blowfish, is perfect for use in embedded systems [2]. Protecting networks needs to be a multi-pronged strategy. Intrusion prevention in the form of strong identification and authentication mechanisms alone are not sufficient [3], [4]. A new solution to help combat this problem is the combination of Intrusion Detection System (IDS) and lightweight but reasonably secure and fast encryption techniques like Blowfish algorithm.

1.1 Attacks and their detection techniques: Attacks could be in the form of jamming the network , Teardrop , Junk transmission thereby draining the batteries of a good node , ping-of-death etc resulting in a DoS (denial of service) attack. Man in the Middle is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them. It makes them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.IDS is a software or hardware tool used to detect unauthorized access of a computer system or network[4],[5]. An IDS usually performs this task in one of two ways, with either anomaly based detection or signature-based detection.

Anomaly Detection: Anomaly detection uncovers abnormal patterns of behaviour. When, it detects deviation in traffic, an alert is generated. The advantage of this system is to catch many attacks that are new or unknown. The drawbacks consist mainly of large amounts of time being spent to train and retrain the IDS system. Also, they produce high amount of false alarms and thus not practically implemented. *Signature or Misuse Detection:* Signature based or misuse detection looks for events that match a predefined pattern. Signature detection relies on the use of specifically known patterns of unauthorized behaviour. Almost every IDS today is at least in part signature-based. Attacks and their tools usually have a unique signature that can be detected and/or found. The known attacks can be detected by looking for these signatures.IDS implementations represent intrusion signatures using specialised languages, including Snort, Shadow, NFR and Bro [7].

1.2 Cryptography Terminology Encryption Algorithms and Hashing Techniques: The process of encryption converts that plaintext message into cipher text, and decryption converts the cipher text back into plaintext. Encryption algorithms come in two flavours, symmetric and public key. Public key encryption algorithms use two keys, one for encryption and another for decryption. The key used for encryption, the "public key" need not be kept

secret. The sender of the message uses that public key to encrypt their message, and the recipient uses their secret decryption key, or "private key", to read it. In a sense, the public key "locks" the message, and the private key "unlocks" it: once encrypted with the public key, nobody except the holder of the private key can decrypt the message. RSA is a popular public key encryption algorithm. Symmetric algorithms, such as Blowfish, use the same key for encryption and decryption. Like a password, you have to keep the key secret from everyone except the sender and receiver of the message. Most credible encryption algorithms are published and freely available for analysis, because it's the security of the key that actually makes the algorithm secure.

Cryptographic hash functions are commonly used to guard against malicious changes to protected data in a wide variety of software, Internet, and security applications, including digital signatures and other forms of authentication. A cryptographic hash function takes any amount of data and applies an algorithm that transforms it into a fixed-size output value. For a cryptographic hash function to be useful, it has to be extremely difficult or impossible to reconstruct the original data from the hash value, and it must be extremely unlikely that the same output value could result from any other input data. MD5, SHA1, SHA256, SHA512 are some of the most standard hash functions used.

Digital Signature -To authenticate the sender of the message it is necessary to attach digital signature with the message. *Digital signatures* are a way to ensure the integrity of a message or other data using public key cryptography and also ensure that the data itself has not been altered. This is like signing a check in such a way that if someone changes the amount of the sum written on the check, an “Invalid” stamp becomes visible on the face of the check. Before a signer can create a digital signature, the signer must first have a digital identity—a public-private key pair and a corresponding digital certificate that proves the authenticity of the signer’s public key. The signer generates a message digest of the data and then uses the private key to encrypt the digest. The signer includes the encrypted digest and information about the signer’s digital certificate along with the message. The combination of the encrypted digest and the digital certificate is a digital signature. Digital Signature Algorithm (DSA) is one of them.

II. RELATED WORK

Gattiff Bill[2], has outlined the importance of blowfish encryption algorithm particularly for data integrity, system security and privacy being light weight and in public domain. Nadeem.A[3], Dhawan.P[4] and Abdul.D.S,Elminaam et.al[5] has specifically stated in their work related to performance analysis of different encryption algorithms that Blowfish outnumbers other algorithms in terms of its comparative execution times and throughput. Uddin M, Khowaja et.al [6] has discussed about the idea of dynamic multilayered signature based IDS. Theuns Verwoerd and Ray Hunt[9] have discussed about various cryptography based IDS approaches. Deepak Dembla et.al have discussed [10] about modelling and analysis of intelligent AODV routing protocol based on request retransmission strategy in MANETS. Yogesh Chaba et.al in their work [11] have discussed about performance analysis of disable IP broadcast technique for prevention of flooding-based DDoS attack in MANETS. Further Yudhvir Singh et.al have described about information theory tests based performance evaluation of cryptographic technique [12]. From the review of literature it was found that many algorithms have been proposed for IDS, but we could not find any work in the literature which has used combination of Digital Signature and blowfish algorithm for any IDS.

III. PROPOSED WORK

Proposed work includes preparation of a security model using Blowfish encryption algorithm, digital signature generation with different hashing techniques like MD5,SHA1 etc. . The sequential approach of the proposed model goes like this:

1. Suppose a packet arrives and is logged in event logs. It is encrypted using blowfish algorithm and its pattern is matched with encrypted pattern database (signature data base) already stored in the system. Signature database is specifically known patterns of unauthorized behaviour. If it matches with the signature database that means it is an attack packet so an alert is generated.
2. If the pattern does not match it is sent for a second stage check Anomaly Detection which is statistical behaviour analysis. If it is not the normal behaviour the signature database is updated to include this new signature.
3. If it shows a normal behaviour then its digital signature (r , s components) are computed and matched, if it matches then packet data is decrypted using blowfish algorithm and if it does not match then system alerts for ‘deny access.
4. This way evasion of IDS may be reduced to some extent at important checkpoints. It involves the use of Blowfish encryption algorithm and computing r,s values using Hashing techniques like MD5 and SHA1, SHA256, SHA512.

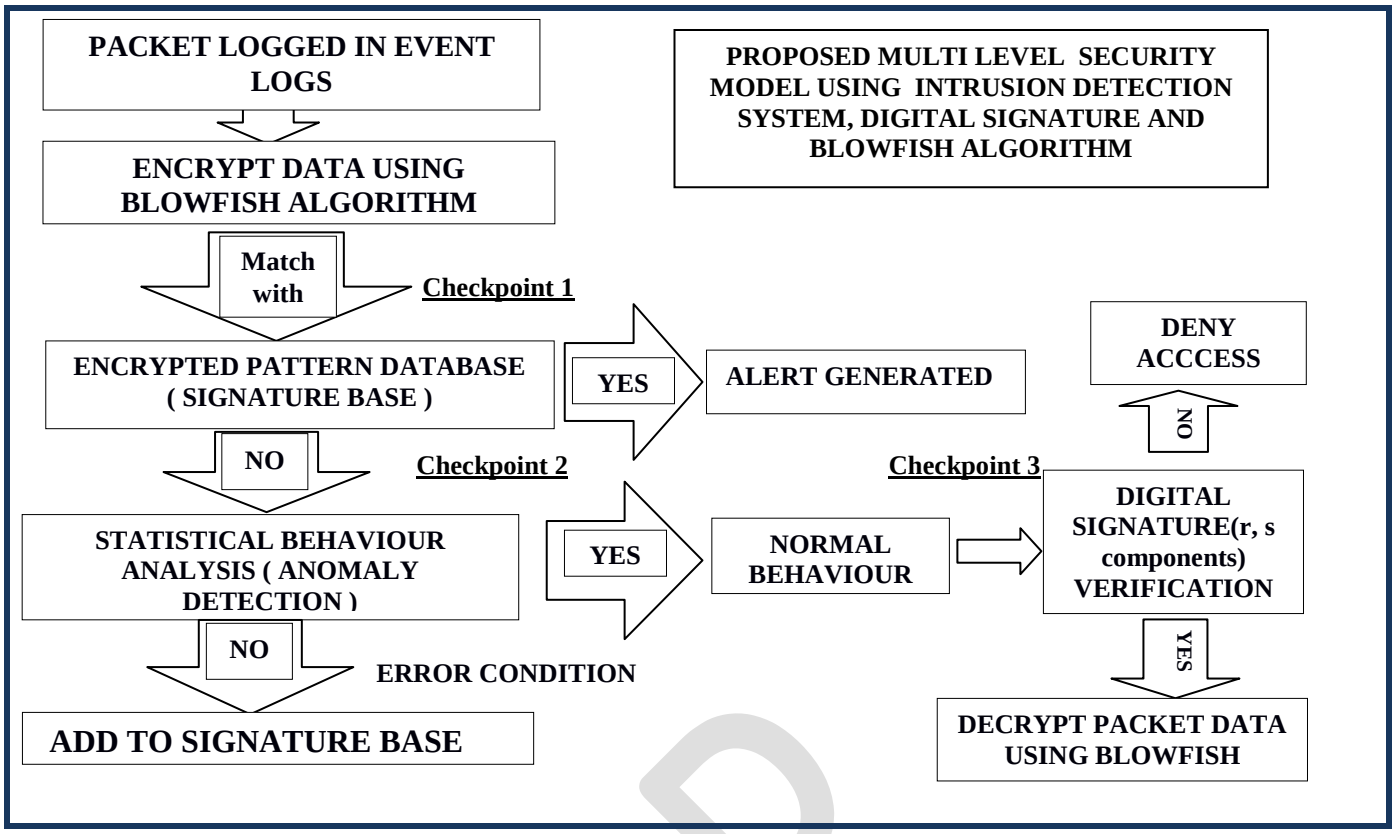


Figure1. Proposed Multi Level Security Model Using Intrusion Detection System, Digital Signature And Blowfish Algorithm

Implementation of The Blowfish Algorithm for proposed system

Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption [1],[2]. The block length for Blowfish is 64 bits; Blowfish is public domain, and was designed by Bruce Schneier expressly for use in performance-constrained environments such as embedded systems [3]. It has been extensively analyzed and deemed "reasonably secure" by the cryptographic community.

In this description, a 64-bit plaintext message is first divided into 32 bits. The "left" 32 bits are XORed with the first element of a P-array to create a value I'll call P', run through a transformation function called F, then XORed with the "right" 32 bits of the message to produce a new value I'll call F'. F' then replaces the "left" half of the message and P' replaces the "right" half, and the process is repeated 15 more times with successive members of the P-array. The resulting P' and F' are then XORed with the last two entries in the P-array (entries 17 and 18), and recombined to produce the 64-bit cipher rtext. Blowfish requires about 5KB of memory. A careful implementation on a 32-bit processor can encrypt or decrypt a 64-bit message in approximately 12 clock cycles. Blowfish works with keys up to 448 bits in length.

The function divides a 32-bit input into four bytes and uses those as indices into an S-array. The lookup results are then added and XORed together to produce the output. Because Blowfish is a symmetric algorithm, the same procedure is used for decryption as well as encryption. The only difference is that the input to the encryption is plaintext; for decryption, the input is cipher text[1][2].The P-array and S-array values used by Blowfish are pre computed based on the user's key. In effect, the user's key is transformed into the P-array and S-array; the key itself may be discarded after the transformation. The P-array and S-array need not be recomputed (as long as the key doesn't change), but must remain secret.

Procedure for computing the P and S arrays is as follows:

P is an array of eighteen 32-bit integers.

S is a two-dimensional array of 32-bit integer of dimension 4x256.

Both arrays are initialized with constants, which happen to be the hexadecimal digits of π (a pretty decent random number source). The key is divided up into 32-bit blocks and XORed with the initial elements of the P and S arrays. The results are written back into the array. A message of all zeros is encrypted; the results of the encryption are written back to the P and S arrays. The P and S arrays are now ready for use[1],[6],[8].

Sub keys:

Blowfish uses a large number of sub keys. These keys must be pre computed before any data encryption or decryption.

1. The P-array consists of 18 32-bit sub keys:
P1, P2,..., P18.
2. There are four 32-bit S-boxes with 256 entries each:

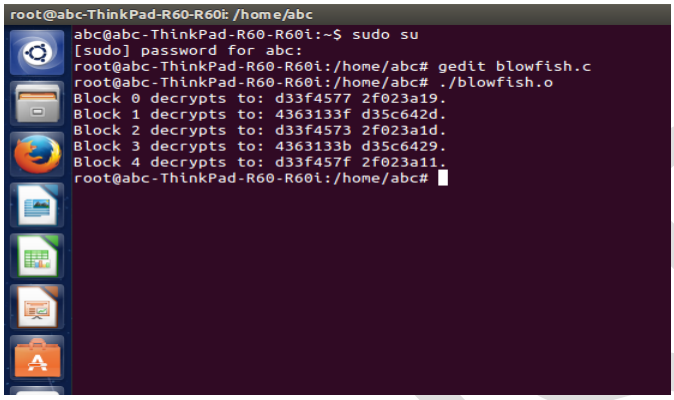
S1,0, S1,1,..., S1,255;
S2,0, S2,1,..., S2,255;
S3,0, S3,1,..., S3,255;
S4,0, S4,1,..., S4,255.

Encryption:
The input is a 64-bit data element, x.
Divide x into two 32-bit halves: xL, xR
For i = 1 to 16:
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR
Next i
Swap xL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR

Function F :
Divide xL into four eight-bit quarters: a, b, c, and d
F(xL) = ((S1,a + S2,b mod 232) XOR S3,c) + S4,d mod 232
Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order.

IV. RESULTS

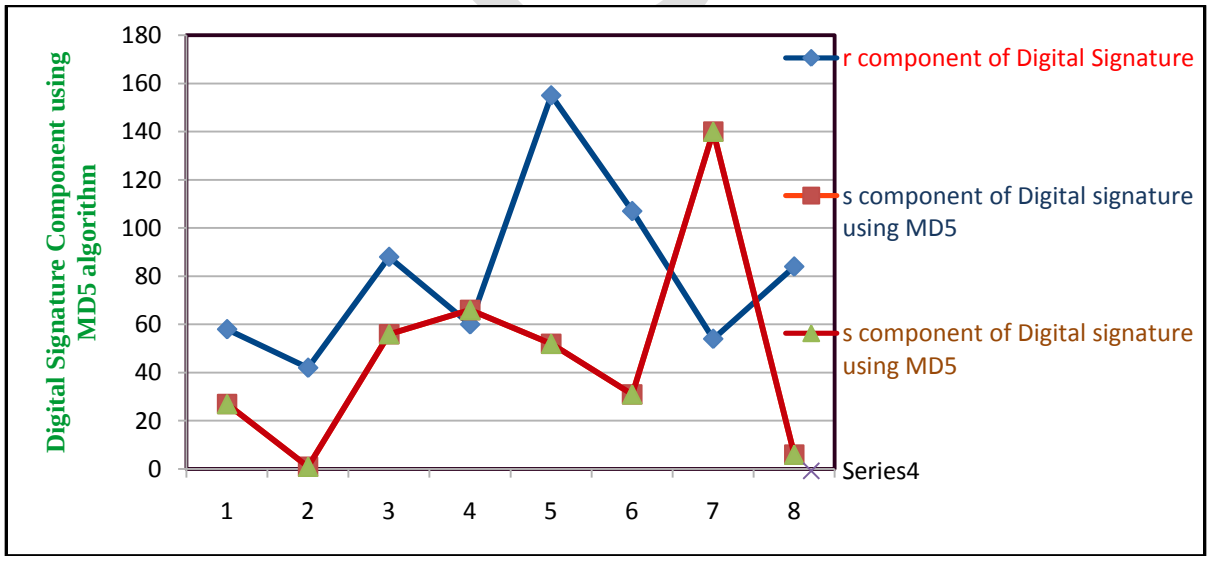
The study so far shows the superiority of Blowfish algorithm over other algorithms in terms that Blowfish algorithm has not any known security weak points so far, this makes it an excellent candidate to be considered as a standard encryption algorithm[5],[6].



Screen shot 1 showing the decrypted values of the data blocks using Blowfish Algorithm

Table 1 showing ' r ' and ' s ' components of digital sinature with MD5 algorithm

r component of Digital Signature	s component of Digital signature using
	MD5
58	27
42	1
88	56
60	66
155	52
107	31
54	140
84	6

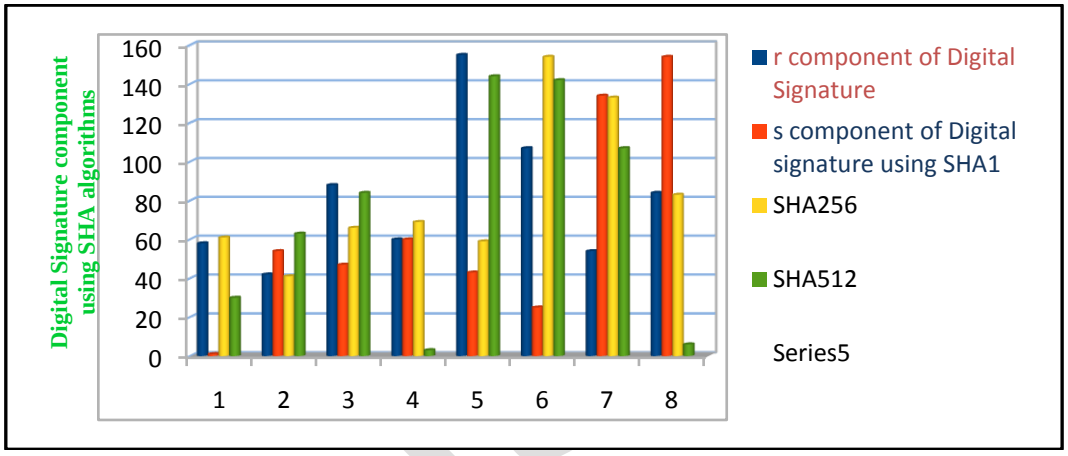


Graph 1 showing ' r ' and ' s ' components of digital signature with MD5 Hashing Technique

The ‘s’ component values in the graph are somewhat(except one) in consonance with the ‘r’ component values and show smooth curves as compared to the message digest values computed with SHA algorithms.

Table 2 showing ' r ' and ' s ' components of digital signature with SHA hashing

r component of Digital Signature	s component of Digital signature using		
	SHA1	SHA256	SHA512
58	1	61	30
42	54	41	63
88	47	66	84
60	60	69	3
155	43	59	144
107	25	154	142
54	134	133	107
84	154	83	6



Graph 2 showing ' r ' and ' s ' components of digital sinature with different SHA algorithms

The values of 'r' and 's' shall be checked to determine if r=0 or s=0. If either r=0 or s=0, a new value of k will be generated and the signature have to be recalculated, however it is extremely unlikely that r=0 or s=0. Values of 'r' and 's' computed in this work also provide valid signature. The signature (r , s) may be transmitted along with the message to the verifier.

V. CONCLUSION

Proposed security model will help in preventing evasion of the deployed IDS. Security of the network system can be enhanced with use of encryption algorithms like Blowfish before an IDS. Study shows that Blowfish and AES have better encryption (i.e. stronger against data attacks) than the other algorithms . Blowfish has an additional advantage over other algorithms in terms of throughput and comparative execution times. It is an excellent choice in combination with digital signature algorithm (DSA) for adding system security , data integrity and privacy capabilities to embedded and other systems being lightweight, in public domain, and considered secure even after extensive analysis. For

Future Work- The proposed model can be improved by using Two fish Algorithm for pattern matching in the intrusion detection system. Better Key length will provide better symmetric algorithm implementation and security. Signatures can be added across databases of multiple IDS systems based on the level of threat to the network.

REFERRENCES

[1] Schneier, Bruce. "*Applied Cryptography: Protocols, Algorithms, and Source Code in C*", Second Edition. New York, NY: John Wiley & Sons, 1995.

[2] Bill Gatiff " *Encrypting data with the Blowfish Algorithm*" RFC , July 2003

[3] [Nadeem2005]Aamer Nadeem , "*A Performance Comparison of Data Encryption Algorithms*", IEEE 2005

[4] [Dhawan2002] Priya Dhawan., "*Performance Comparison: Security Design Choices*," Microsoft Developer Network October 2002.

[5] Abdul D S, Elminaam, Kader H M A and Hadhoud M M (2008), "*Performance Evaluation of Symmetric Encryption Algorithms*," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December.

[6] Uddin M, Khowaja K and Rehman A A (2010), "*Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents*", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October.

[7] Sen J (2010)," *An intrusion Detection Architecture for Clustered Wireless Ad Hoc Networks*", Second International Conference on Computational Intelligence, Communication Systems and Networks.#

[8] Stallings W (2005), "Cryptography and Network Security, Principles and Practices" Pearson Education, New Delhi

[9] Theuns Verwoerd and Ray Hunt, "*Intrusion Detection Techniques and Approaches*", Newzeland

[10] Deepak Dembla, Yogesh Chaba, "Modeling and Analysis of an intelligent AODV Routing Protocol based on Route Request Retransmission Strategy in MANETs" *International Journal of Computer Applications* (0975-8887), Vol. 30, Issue 11, pp. 6-13 (2011)

[11] Yogesh Chaba, Yudhvir Singh, Preeti Aneja, "Performance Analysis of Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET" *Journal of Networks*, Vol 4, Issue 3, pp. 178-183 (2009)

[12] Yudhvir Singh, Yogesh Chaba, "Information theory tests based performance evaluation of cryptographic techniques" *International Journal of Information Technology & Knowledge Management*, Vol. 1, Issue 2, pp.475-483 (2008).