EFFICIENT KEY MANAGEMENT AND AUTHENTICATION USING ENHANCED IDENTITY-BASED CRYPTOGRAPHY FOR SECURE SMART GRID COMMUNICATIONS

Joshila Grace.L.K.

Assiatant Professor, Department of CSE, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India.

joshilagracejebin@gmail.com

Abstract: **The more attacks have been increased over the network and other related system is also being increased for harming the internet and network, the defending system are outdated and outnumbered for protecting the system. The attacks are become dangerous and make more harm to the network or internet. The proposed technique is presenting an enhanced and efficient way within the algorithm of unique cryptography and public key for protecting the network or system and preventing the attacks. The policy and scheme are playing a very important role for making a communication within several clients by using common channel. There are several attacks are existing internally or externally when creating communication over the proposed technique, proposed techniques are completely able to defend or prevent the attacks and reduce the management stress. The accuracy and efficiency are being improved within the proposed technique through the key management policy which has broadcasted the key generation and update the multicast, public and personal key in each node. Proposed system are presenting the polynomial algorithm for reducing the flow of message bulk, Hash-Based algorithm and Cryptographic algorithm for processing over the high speed data processing.**

Keywords**: Cryptography, Identity-based cryptography and key distribution algorithms.**

1. INTRODUCTION

The information and network security are often interchangeably and known for the protection from hackers, security form several virus attacks and intrusion. The term information security is completely making focus on protection of several attacks of malware and few mistakes from the user or organization within prevention of loss of data [1]. Some of these techniques are for collage of huge networks in internal boundaries. In internet world, the network security is playing an important role for protecting the information and travelling of the stored data against of data modification and unauthorized disclosure that seems about the occurrences of accident such as improper debugging program application which is making a damage of data. There is different way for consider the differences amid of privacy and security. The security or privacy is a complete need for every user to prevent the data accessing, whether it trading the personal or secret data trading have to be secret by the law. The security is being considered for maintaining the privacy. The network securities have three major goals:

Confidentiality: surety of privacy and security,

Integrity: surety for data accuracy. Prevention of unauthorized accessing of data,

Availability: accessibility right of data whenever organization wants.

External threats sources

The internet services have been considered in both sides as of the positive and negative effects for those users or organization whose business is running on network or internet supply. The worldwide network of internet has through it feasible for probable consumer, employees, and users to attain an association throughout their Web site. However within it the novel admission have become the mammoth troubles caused by particulars and grouping to attempt illegal access in networks or internet and the support or system [2][3].

External Crackers and Hackers coercion are started by known people for community of hacking as hackers or crackers. Generally, the hacker term considered to someone who can break the security system writing a program or unique code that can make possible for any impossible access in to possible. In fact, the expression “perfect hack” meant to a individual smart programming [3][4]. External part for community of hacking, but, anyone try to attempts unauthorized accessing of network or system is known as hacker [3][6]. Hacking frequently engaging get attached with every details of intimation for existing software for providing a necessary knowledge for unauthorized to break all the security system. A hackwer is completely different in compare to a normal programmer who could break the security system for any software [6].

There are several techniques and methods for identifying them who can provide a accessing right to any unauthorized user, this is completely different and depending ways to make read the system a different way of code. There are some types of hacker mentioned below:

- ✓ Script Kiddie
- ✓ White Hat Hackers
- ✓ Black Hat Hackers
- ✓ Cyber terrorists

Attack Types

There are several categories mentioned for attacks:

DOS (Denial of service):

The DOS try to access illegally for collecting the information and data by damaging the security system of networks and internet resources. It is making a flood over the network to get access by creating heavy traffic on the network, Denial of service is feasible to get identify or detect. But it’s not possible to prevent the accessing without disconnecting the network.

Overflows of Buffer:

The attack of Buffer overflow is taking advantage over error of programming in system program or application. The hacker could insert the code into a system program for taking complete control. The attack by buffer flow is approx impossible to get identified [3][9]. The majority common and working defense is providing patch by the vendors.

Malware:

The malware contain every kinds of nasty software, like Trojan horses, viruses, and worms. The aim of an intruder is for placing worms or virus on the computer system to get access of computer data from the internet or network sources without authentication. Anyway, there are several anti-virus are existing for defending the system from this all types of attacks [2].

Social engineering:

It is a fake advertising process that attracting the internet users to handover all the information foolishly without knowing about the service provider reliability. It is not a technical stuff for accessing the information and data from another system [5]. By using some common sense, there is a way to prevent this types of attacks.

Brute force:

This is also an technique or fake methodology for gaining the access right, if the hacker or attacker knows several system login names they can try to access the system by guessing the password [9][10]. By using log or user access and authentication process, these attacks could be possible to prevent.

2. LITERATURE REVIEW

The BGP routing protocol Security. Recognize vulnerabilities in design and respective corresponding threats. The proposed modification protocols eliminate or minimize the significant threats. The security over the information is of second-to-last path of AS PATH within digital signature. The use of development technique could be able to identify the loops in protocols of path-findings for verifying the selected path. The security over full path is about to space constant and for avoiding the protection mechanism [1].

The S-BGP (Secure Border Gateway Protocol) is the Real World Deployment and Performance Issues [2].

The Frontier portal Protocol is being used for distributing the information between autonomous systems that is completely important system over the infrastructure of internet routing. The routing address of the S-BGP vulnerabilities provides a scalable meaning of BGP authorization and authenticity for traffic control. S-BGP ought to evade establishing unnecessary slide (storage, bandwidth, processing) and should be deployable. S-BGP deployment and execution in DARPA’s CAIRN is being tested. The Real sources of Internet traffic was feed for the verified routers through recorded BGP replay session of peering session with BGP router.

The Understanding of BGP Misconfiguration is allowing Accidental configuration errors of BGP that could disrupt the connectivity of Internet [3].

The Implementation of Economical and Small-Sized HMAC (Keyed-Hash Message Authentication Code) is making small-sized high-speed implementations of the skittish-Hash Message Authentication Code is conferred.

The implementation process could be either in HMAC-SHA1 or HMAC-MD5 mode.

The process of implementation is not introducing any significant penalty area. The comparison of commercially available IP cores the range between 30-390%.

The beneficiation of this paper is to increase the throughput of HMAC over the required level of enhanced technology or applications like oncoming 802.11N and VPN.

Encryption Key Exchanging: the process is established on the password within dictionary protocols [4]. The classical protocols of cryptography are based on the selected keys that allow an attacker to extract the password by guessing.

The novel combination of public key and private key cryptography

This is allowing the two systems to get communicate by exchanging the password secretly and authenticates the user to get information over insecure network. The securities against active attacks are having a property that could protect the password against of the dictionary attacks.

There are several useful applications as well that includes the public telephones [5].

3. SYSTEM ANALYSYS

The aim of this system is to identify the feasibility of study for finding the perfect resolution for solving the problems within several schemes and options for identifying the way for system design. The system have three major factors for feasible study:

1. Technical feasibility
2. Operational feasibility
3. Economic feasibility

A. Modules

The below mentioned terms are the modules that is related to the projects for implementation that is planned to execute within proposed system when processing within the existing system and also transfer backing for the intensify the service in future. There are completely five modules mentioned below:

- Login/New User
- Sender/File Transmission

- Key Generation
- Key Management
- Hacking Zone/Monitoring

Sender/File Transmission:

This module is describing the process of login for the security reason. The username and password is the required field for the validation and authentication within some additional action is performing the and providing the security within login.

The process is allowing user to register within the server and database by using username and password through validation and set of key is being generated for authentication [12] [14].

This module is allowing the user to select the file for sending to the different users. The creation of new users are processing over entitle of the collecting information for maintaining the key transferring. The key has been generated in database is acting as OTP.

Signature (Key) Generation:

The sender or the owner is holding the signature for generating the key, which is divided into two parts as public key and private key for providing additional security over the conveyance of data. The private key is allowing the sender to send the particular selected data to a particular location. The public key is allowing the user to send the data to all the receiver or users on the networks [5], [11].

Table 1: Modules Interaction

Module Name	**Input**	**Output**	**Techniques**
Network Authentication	**User Details**	**Sender Frame**	**JDBC Connection**
Sender/File Transmission	**Key and File**	**Data transferred**	**Encryption & decryption**
Key Generation	**Registration phase**	**Keys will be generated**	**HMAC SHA1 Algorithm**
Key Management	**Set of Keys from the Database**	**Elective key from the Set of keys**	**One Time Authentication**
Attack Identification	**Virus Files**	**Blocking the virus**	**Chaos Theory**
Hacking/Monitoring	**Hackers on Network**	**Data extraction from the network**	**Pandora FMS, Fiddler, Capsa Free, etc…**

Signature (Key) Management:

The signature management is having two mechanisms for symmetric key that is pre-key distribution and consolidates key distribution.

1. Pre-Key distribution :

The users are provided a substantial number that avoid the frequent generation of updating of key. The periodic generation technique of key is being changed within every period of time which long sufficiently [13]. The individual router is completely responsible for key generation.

2. Centralized Key Distribution:

- The central authority or manager is responsible for the generation of key.
- This approach is generating the cost signature for router within one signature.
- The signature cost is lower.
- The router is only adding the self signature by updating their signature, the cost is low.

Hackers Zone

The different network node is or any particular system is accessing the data from existing network is accessing the data from false node name and collecting the information from other router is known as hackers [3] [8] [12]. The random generated key is not allocating to the hacker system.

- ***Monitoring Access***

The module of monitoring system is taking care for sending the data by using network key. It is accessing the database for checking the proper validation for invalid or valid users. It is monitoring the hacker's activity and trying to access the information or data which is not belongs to network.

Receiver:

Some intersections are behaving as sender and receiver and every remaining node are receivers.

If any node is sending the message which is having the signature for every keys and verifying the signature by using similar key and authenticate the message.

SYSTEM ANALYSIS

The analysis of system is defining process of intellectual break down or whole substantial parts. The procedure of union is defining the procedure of separate element combination or components order for coherent process.

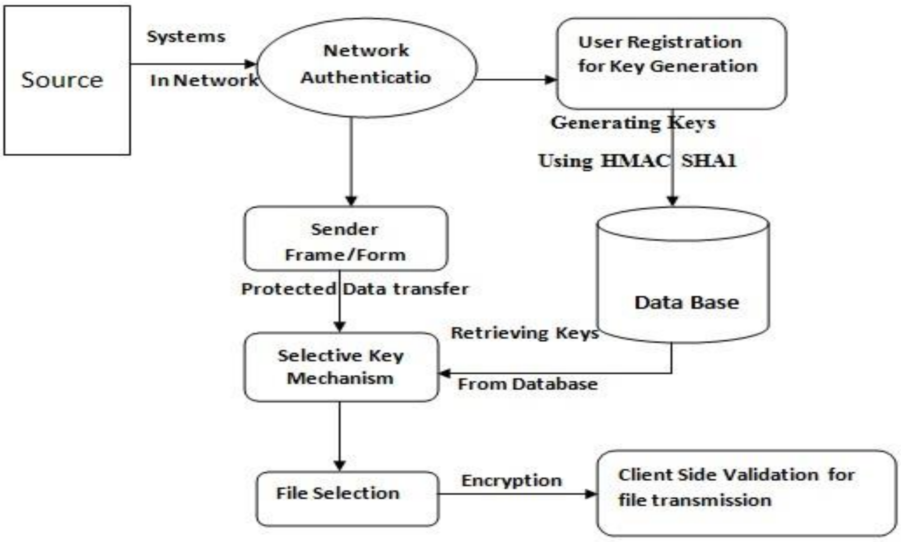
A. Existing System

- The existing network structure is providing the insecure mechanism.
- There are no other techniques or schemes available for WSN in real world application for large scale.
- The solution of the existing system is presenting the trade-off functionality over the security and performance.
- The identification of basic structure of building is describing the details of solutions.

Drawbacks of the Existing System

- It is increasing the group manager workload.
- It is creating the heavy network traffic by exposing the traffic analysis risk.
- It is too easy to determine the reused mechanism for several of solutions.

System architecture block diagram



B. Proposed System

- The scheme of functionality is decomposing the three aspects, namely: self-invigorating mechanism, distribution mechanism and pre-distributed management of secret data for classification and scheme of compare.

- The proposed techniques are addressing a security metrics within SG system at same time and managing the process in enhanced formation.

- The consumption of resources is being saved as mechanism result which could be able to handle more delivery of data and increasing the system security by random generation of key.

- Conveyance dependability is achieved by message encryption and authentication using shared symmetric secret group key.

Advantages of the Proposed System:

- Technique or scheme for distributing the key could satisfy.
- It is preventing the unauthorized user to access by learning group key.
- More flexibility.
- It can be used in multi-cast networks with centralized management.
- Key giveout perspective has to provide fresh keys.

4. CONCLUSION

The proposed methodology is contributing three major process that showing the concession amid of security and efficiency over information that could be achieved through adding small trust point over routers. The methodology is presenting the comfortable threat module for “k” length path within trustworthy router.

Secondly, the methodology is presenting novel key approach for generating the symmetric key for information security: the approach of distribution Consolidate key and approach for distributing distributed key. Third, the efficient approach for fortify of data. The result is showing better approaches for more significant approaches. The methodology is discussing issues of deploy and key administration and illustrate interoperability for feasible protocols.

5. FUTURE WORK

The critical steps of the criss-cross and internet security is being discussed in the proposed methodology that have been producing better enhancement but the attack on network or internet is too fragile and wouldn’t be stop to go for the more better enhancement.

The IETF (Internet Engineering Task Force), ISPS and organization of registration will need to invest more amount on the novel and enhanced technology. In this case, the organization would be interested to implement digital signature (PKI) Public Key Infrastructure without spending more amount and buying ISP that will be saving amount and time.

REFERENCES

[1] Adams, C., and Tavares, S. "Generating and counting binary bent sequences." IEEE Transactions on information theory, 1990.

[2] Adams, C. "Simple and effective key scheduling for symmetric ciphers." Proceedings, workshop in selected areas of cryptography, SAC' 94. 1994.

[3] Adleman, L. "The function field sieve." lecture notes in computer science 877, Springer- Verlag, 1983.

[4] Agrawal, M.; Keyal, N.; and Saxena, N. "PRIMES is in P." IIT Kanpur, Preprint, August 2002. http://www.cse.iitk.ac.in/news/primality.pdf

[5] Akl, S. "Digital signatures: A tutorial survey." computer, february 1983.

[6] Alvare, A. "How crackers crack passwords or what passwords to avoid." Proceedings, UNIX security workshop II, august 1990.

[7] A.Viji Amutha Mary, SJ Samuel, DJ Rajam, "Automated Trinity Based Web Data Extraction for Simultaneous Comparison" Contemporary Engineering Sciences 8 (11), 491-497, 2015.

[8] Audin, G. "Next-Gen Firewalls: What to Expect." Business Communications Review, June 2004.

[9] Axelsson, S. "The Base-Rate Fallacy and the Difficulty of Intrusion Detection." ACM Transactions and Information and System Security, August 2000.

[10] Bace, R. Intrusion detection. indianapolis, IN: Macmillan technical publishing, 2000.

[11] Bace, R., and Mell, P. Intrusion Detection Systems. NIST Special Publication SP 800-31, November 2000.

[12] Mercy Paul Selvan, R Selvaraj "Monitoring Fishy activity of the user in social networking". 2017 International Conference on Information Communication and Embedded, 2017.

[13] Barreto, P., and Rijmen, V. "The Whirlpool hashing function." Submitted to NESSIE, september 2000, revised May 2003.

[14] S.P. Godlin JasilV. Mani, "An efficient bundle range aggregation using R-Tree", International Journal of Applied Engineering Research, 2015