DATA PRIVACY IN SMARTPHONES USING TIME HOMOGENEOUS MARKOV CHAIN MODEL

Dr.P.Maragathavalli and G.Hemalatha

marapriya@pec.edu, ghema207@pec.edu

***ABSTRACT*-Smartphones bring users to save many confidential data such as personal photographs and video, access to bank accounts on their mobile devices. These devices are being connected to the internet and thus vulnerable to online attacks. In smartphones there are many serious security issues which need to be addressed. The major security problems are multimedia data theft, cyber-attacks such as double locker and injecting malicious code. This paper addresses the issues of protecting sensitive data including video from unauthorized users. In existing methods for data protection require more storage space and computational time. In order to reduce storage as well as time, Time Homogeneous Markov Chain Model (THMCM) has been introduced. The proposed system includes a concept of time restriction for accessing the confidential data in markov chain model.By generating fake data instead of sensitive information, the original data is protected from attackers in cloud environment. In THMCM, the trigger module decides either to provide original content or fake which in turn givesaccess permission to view the hidden volume.The proposed model restricts the unauthorized users to learn the output sequence of the contexts in sensitive data of the user and provide the cloud storage backup for sensitive data to store and retrieve using Elliptic Curve Cryptographic (ECC) algorithm.**

Keywords: Sensitive data, Cyber-attacks, unauthorized user, Cloud storage, Hidden volume.

I.INTRODUCTION

The smartphone usage raised significantly in recent years, as smartphones provide users with several services like phone calls, Internet services, sharing data, keeping data, off-line games, online games, and some entertaining online/ off-line applications. As smartphone provides the vast services, thus are saddled with some challenges like security and privacy as well. Since most of the operations smartphones perform are on the Internet, so it is necessary to ensure security and safety of data and information. For example, the non-public sensitive information and the location trace of an individual could also be sold-out by a smartphone application to a poster server, which can cause a threat to the user's privacy and even life safety. Therefore, individuals have associate degree increasing demand for reducing the chance of context revealing whereas enjoying those context-aware services.

For privacy protection, a several of privacy preserving techniques have been proposed, most of deals with location privacy. For more complex policies are adopted to increase the difficulty of inferring sensitive contexts in privacy preserving smartphone applications. A deception policy is used in location privacy preserving approaches in which fake location information is released if the current location information is sensitive and should not be exposed to untrusted applications. As aforementioned above, human contexts have high temporal correlations, and the previously released contexts could be used by an adversary to infer the current context, thus increasing the risk of privacy disclosure.In mask italong with the non-sensitivedata, sensitive data may be suppressed to decrease the temporal correlations among contexts.

II.PRIVACY ISSUES IN SMARTPHONES

Smartphones have features of both a mobile phone and a computer, allowing us to talk, text, access personal and work e-mail, browse the Internet, make purchases, manage bank accounts, and take pictures. They are becoming capable of doing more and more every day. Unlike many of our computers, our smartphones are always with us and many of

us rarely turn them off. However Fig.1 shows the various privacy issues in smartphones consumers need to be aware of the kind of information that can be collected by various entities from your smartphone.

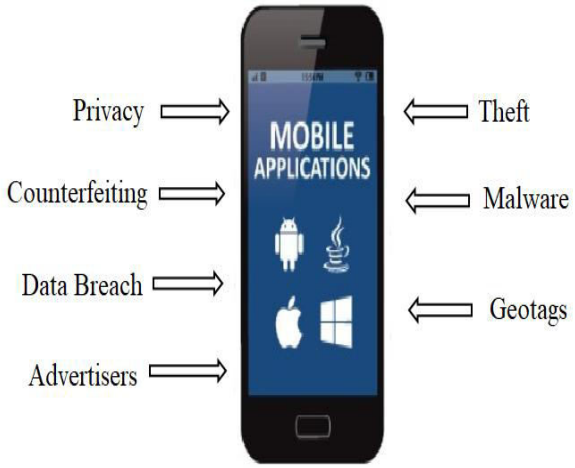

Fig. 1 Privacy Issues in Smartphones

Criminals

A cybercriminal may want to: steal your money, collect personal data to commit identity theft, harass or stalk you. To further their goals, cybercriminals may try to steal your phone or find ways to use your smartphone to snoop on you through malware or public Wi-Fi networks.

Theft:Smartphones store a tremendous amount of personal information. If your smartphone were lost or stolen, what information would someone be able to access?

Malware: Malware refers to all categories of malicious software, and poses a threat to your smartphone just as it does to your computer. The term "malware" includes viruses, spyware, Trojan horses, worms, and basically any other harmful software or program. The apps on your smartphone are a common avenue for transmitting malware. However, malware may also be distributed through advertising and upgrade attacks as well. Unfortunately, mobile malware attacks are on the rise in part because individuals are less likely to guard their smartphones in the way they do their computers. Also, attacking a smartphone may provide criminals with quick rewards because the increasing popularity of mobile payment options allows criminals to directly profit off of their attack. Criminals can also profit by directly charging to an individual's phone bill.

*Geotags:*Depending on the settings, your smartphone may be using its built-in GPS capability to embed your exact location into the file of photos you take using the smartphone's camera. The process of embedding location information into photos is called geotagging. If you share your photos and they end up on the Internet, criminals can use the geotag to track your movements or find out where you live. Note that Facebook automatically strips out geotags, so any photos posted to Facebook do not have your location embedded in the file.

Advertisers

Advertisers want to market to the people who are most likely to buy their product or service. The more information they collect about you, the better their ability to know the types of products and services you are most likely to buy. Currently, applications (or apps) are widely-used by advertisers to capture your smartphone data. The privacy concern here is that information could be shared with third parties and compiled with other data to create a detailed profile about you without your knowledge or consent.

Mobile Application: Advertisers pay app developers to get access to you. The advertisers supply code to the app-makers to build into the app. The code not only makes an ad appear when you use the app, but also collects data from your phone and transmits it back to the advertiser. It's also possible that the app itself collects data which is shared with ad networks. The ad networks may then show the user ads that contain content based on the data collected.

Behavioural Marketing or Targeting:Behavioural marketing or targeting refers to the practice of collecting and compiling a record of individuals' activities, interests, preferences, and/or location over time. This data may be compiled, analysed, and combined with information from offline sources to create even more detailed profiles.

The ability to collect data on where a person has gone and what they have been doing is valuable information for law enforcement officers.

III.LITERATURE REVIEW

1. Wei Wang and Qian Zhang, 2016 "Privacy Preservation for Context Sensing on Smartphone"

The main goal is to identify the context privacy problem with consideration of the context dynamics and malicious adversaries with capabilities of adjusting their attacking strategies and formulate the interactive competition between users and adversaries as a competitive Markov decision process (MDP), in which the users attempt to preserve the context-based service quality and their context privacy in the long-term defense against the strategic adversaries with the opposite interests. They Consider the distinct features of context privacy problem including the context dynamics and adversaries with knowledge of temporal correlations between contextsand capabilities of adjusting their attacking strategies, we formulate the interactive competition between users and adversaries as a competitive MDP, in which the users aim to maintain the context-based service quality and their context privacy by deciding the data granularity of each sensor that are accessed by the context-aware applications. The adversaries adjust their strategies on which sensing data are selected as the source to launch attacks. An efficient minimax learning algorithm used to obtain the optimal policy of the users and prove that the algorithm quickly converges to the unique Nash equilibrium point

2. BilalShebaro, OyindamolaOluwatimi, and Elisa Bertino, 2015 "Context-Based Access Control Systems for Mobile Devices"

They propose a modified version of the Android OS supporting context-based access control policies. These policies restrict applications from accessing specific data and/or resources based on the user context. The restrictions specified in a policy are automatically applied as soon as the user device matches the pre-defined context associated with the policy. This approach requires users to configure their own set of policies; the difficulty of setting up these configurations require the same expertise needed to inspect application permissions listed at installation time. They have modified the Android operating system so that context-based access control restrictions can be specified and enforced.

3. A. Skillen and M. Mannan, 2015 "Mobiflage: Deniable Storage Encryption for Mobile Devices"

Mobiflage enables PDE on mobile devices by hiding encrypted volumes within random data in a devices free storage space.They leverage lessons learned from deniable encryption in the desktop environment, and design new countermeasures for threats specific to mobile systems.They provide two implementations for the Android OS, to assess the feasibility and performance of Mobiflageon different hardware profiles. MF-SD is designed for use on devices with FAT32 removable SD cards. Our MF-MTP variant supports devices that instead share a single internal partition for both apps and user accessible data. MF-MTP leverages certain Ext4 file system mechanisms and uses an adjusted data-block allocator.

4. W. Wang and Q. Zhang, 2014 "A Stochastic Game for Privacy Preserving Context Sensing on Mobile Phone"

They identified the context privacy problem with consideration of the context dynamics and malicious adversaries with capabilities of adjusting their attacking strategies, and then formulate the interactive competition between users and adversaries as a zero-sum stochastic game and an efficient minimax learning algorithm to obtain the optimal defense strategy. To consider the distinct features of the context privacy problem including the context dynamics and powerful adversaries with knowledge of temporal correlations between contexts and capabilities of adjusting their attacking strategies, they formulate the interactive competition between users and adversaries as a zero-sum

stochastic game. To obtain the user's optimal defense strategy efficiently, a minimax learning algorithm used to solve an equivalent problem with reduced dimensions.

5. M. Gotz, S. Nath, and J. Gehrke, 2012 "Maskit: Privately releasing User Context Streams for Personalized Mobile Applications,"

MASKIT is the first approach to preserve privacy against the adversaries who know the temporal correlations among the contexts. In MASKIT, the temporal correlations among a user's contexts are modelled by a time-heterogeneous Markov chain, which is supposed to be observed by an adversary. By suppressing more contexts than the naive approach, MASKIT tries to maximize the number of released contexts with privacy preservation. Although the user's privacy is guaranteed in MASKIT, the number of released contexts of a user is less than that in the naïve approach. In MaskIt, not only sensitive contexts but also non-sensitive contexts may be suppressed to decrease the temporal correlations among contexts. Since some non-sensitive contexts together with the sensitive ones are hidden.

6. WilliamEnck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, Anmol N. Sheth, "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones"

An efficient, system-wide dynamic taint tracking and analysis system capable of simultaneously tracking multiple sources of sensitive data. TaintDroid provides real-timeanalysis by leveraging Android's virtualized executionenvironment. TaintDroid, an efficient, system-wide information flow tracking tool that can simultaneously track multiple sources of sensitive data. A key design goal of TaintDroid is efficiency, and TaintDroid achieves this by integrating four granularities of taint propagation (variable-level, message level, method-level, and file-level) to achieve a 14% performance overhead on a CPU-bound micro benchmark.

From the literature review, we conclude that all the existing work supress both the normal data and sensitive data or else it release the normal data along with sensitive data. Hence we proposed the system where sensitive data are protected and fake data are generated to the intruder.

IV. PROPOSED SYSTEM

The main motivation of this system is to protect the sensitive data from the intruders using time homogeneous markov chain model which limits what the intruders can learn from the output sequence of contexts about the user being in sensitive contexts even if the adversaries are powerful enough to have the knowledge about the system and the temporal correlations among the contexts. It enables a trigger strategy to delete sensitive data. The proposed system provides a backup in cloud storage for privacy preserving purposes. Sensitive data and images are stored and retrieved using ECC algorithm. As Fig.2 shows the architecture of proposed system.

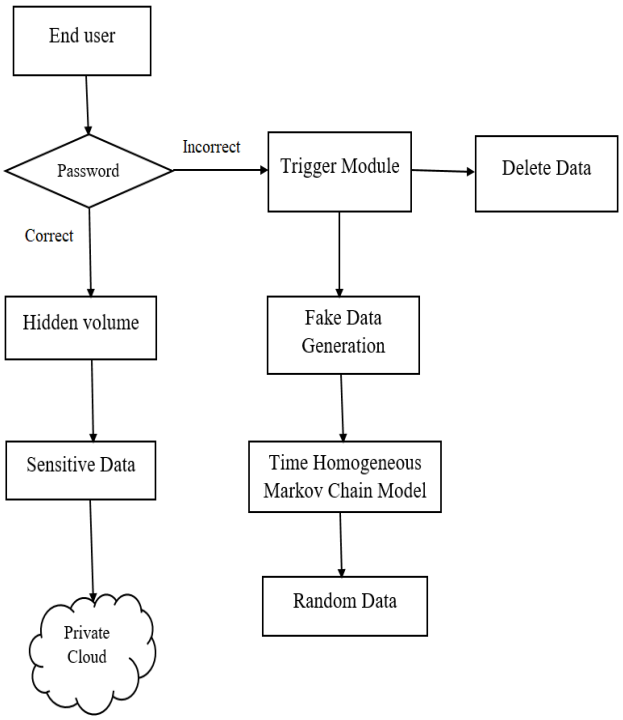

Fig.2 Architecture of theproposed system

The Proposed system consists of three modules namely Trigger module, Generate fake data to intruder and Data storage and retrieval in cloud.

1. Trigger Module

The module builds a trigger strategy. When the trigger condition is satisfied, corresponding actions will be performed. The module listens to a broadcast to capture the device state. To better prevent leakage of sensitive data, the secure defense is divided into three levels. The leakage probability of the sensitive data is in turn increased from level one to level three.

The first level denotes that the mobile device is suffering the most serious threat, such as an adversary capturing the mobile device .When the number of inputs of a wrong password reaches at three, the operating system will unmount the hidden volume.

In the second level, after third attempt if the user enters an application, he/she has to enter the password for the hidden volume to view the sensitive data. If the given password is correct, then it shows the original sensitive data otherwise it generates fake data and send it to the user.

In the third level, when the number of failed attempts to unlock the screen reaches five, the operating system will unmount and then delete the hidden volume. The trigger strategy not only prevents leakage of sensitive data but also ensures deniability of our prototype system.

2. Generate Fake Data to Intruder

After third attempt if the user enters an application, he/she has to enter the password for the hidden volume to view the sensitive data. If the given password is correct, then it shows the original sensitive data otherwise it generates fake data and send it to the user.

A. Markov Chain Model

Markov chains are a fundamental part of stochastic processes. They are used widely in manydifferent disciplines. A Markov chain is a stochastic process that satisfies the Markovproperty, which means that the past and future are independent when the present is known.This means that if one knows the current state of the process, then no additional informationof its past states is required to make the best possible prediction of its future. This simplicityallows for great reduction of the number of parameters when studying such a process.

In mathematical terms, the definition can be expressed as follows:

A stochastic process $X = \{Xn, n \varepsilon N\}$ in a countable space S is a discrete-time

Markov chain if:

For all $n \geq 0$, $Xn\varepsilon S$

For all $n \geq 1$ *and for all* $i_0 \ldots i_{n-1,}$ $in \varepsilon S$,

$$P\{X_n = in \mid X_{n-1} = i_{n-1}, \ldots, X_0 = i_0\} = P\{X_n = i_n \mid X_{n-1} = i_{n-1}\}$$

--- (1)

Markov chains are used to compute the probabilities of events occurring by viewing them as states transitioning into other states, or transitioning into the same state as before.

B. Time Homogeneous Markov Chain Model

Time-homogeneous Markov chain in which the future state is only determined by the present state. That is, a user enters a state next time only based on the user's present state and the transition probability. Formally, whenever the process is in state *i*, there is a fixed probability $P_{i,j}$of which it will enter state *j* next time.

In a Markov chain or a time-homogeneous Markov chain, a user may dwell at a state for some time. The main difference between them lies in the independence property of Markov chain. In the former, a state denotes a context at a time instant, and the transition probability $P^{t}_{i,j}$denotes the probability of the user being in context *j* at time $t + 1$ under the condition that the user was in context *i*at time *t*. That is, the independence property of state transitions is related to the present time. Formally, whenever the process is in state *i*at

time t, there is a fixed probability $P^{t}_{i,j}$of which it will enter state j at time t+1. In contrast, in a time-homogeneous Markov chain, the independence property of state transitions is different. In a time-homogeneous Markov chain, the conditional distribution of any future state X_{n+1}, given the past states $X_0, X_1, \ldots, X_{n-1}$ and the present state X_n, is independent of the past states and depends only on the present state and the dwelling time at the present state.

From the analysis, we can say that the same scenario with temporal correlations among states, if a time-homogeneous Markov chain Model (denoted by Z) is used, the storage consumption is less than that in the case where Markov chain Model(denoted by Z_1) is used. A time-homogeneous Markov chain Z use less the storage consumption than a Markov chain Z_1. The numbers of random variables in Z and $Z_1$are the same, and that the numbers of the different states in Z and $Z_1$are also the same. But, the numbers of the state transition probabilities that should be stored in smartphones are different. Suppose one day is divided into T time periods in each of which a context is sensed, and there are N states in total. We can get that the number of the state transition probabilities required by $Z_1$is $T \times N \times N$. However, the maximum number of state transition probabilities required by Z is $M \times N \times N$, where M is maximum number of dwelling time units for the user. Since a user may dwell on one state for some time, the number of the state transition probabilities required by Z can be greatly decreased. Furthermore, we have $M << T$, leading to less storage consumption for state transition probabilities required by Z.

C. Semi-Markov Chain

A semi-Markov chain is defined as a process $\{X_n, n = 1, 2, \cdots\}$, in which each time the process enters state $i$it dwells there for a random amount of time and then makes a transition into state j with probability $P_{i,j}$. If the dwelling time at a state is independent with the time at which the process enters that state, such semi-Markov chain is time-homogeneous; otherwise, it is time-heterogeneous. Specifically, with the condition that j is the next state, the state dwelling time at state $i$has the distribution $F_{i,j}$. That is

$$Fi,j(t) = \Pr\_[Hi = t | X_1 = i, X_2 = j]$$

$$= \Pr\_Hi = t | X_1, \ldots, X_k = i, X_{k+1} = j], \text{---(2)}$$

Where Hi is the state dwelling time variable of the process in state i.

D. Privacy Checking Algorithm

Privacy checking algorithm that generates an emission probability $b_{i,j}$of state $i$changing to state j. We suppose that a user is in context $i$currently. The context-aware applications cannot access the current context $i$of the user directly and only can collect the context from the system. The output context of the system is determined by the emission probability $b_{i,j}$, which means context j is the output with the probability $b_{i,j}$. We should mention that the generated context is also from the set of contexts that the user may dwell at. The generated context still has some meaning, which means that the user may dwell at that context. Thus, at different time a user may be in the same state, but the output states may be different. Among all the vectors of emission probabilities b that preserve δ-privacy, we seek one with the maximum utility. To approximate the real scenarios of smartphones mentioned in the former section, we assign different weights to the contexts of a user, $W = \{w_1, \ldots, w_n\}$, in which $w_i \in [0, 1]$ denotes the weight of context ci and the sum of all the weights equals 1. Thus, the weighted expected number of released actual contexts is the measurement of the utility U (b).

$$\delta = U(b) = \sum_0 wi \Pr[0].|\{i|oi = C_i\}|$$

$$= \sum_{t \in [T], i \in [m]} wi \Pr[Z_t = c_i] b_{ci,ci} \text{---(3)}$$

Where δ = privacy parameter

A user determines each weight $w_i$for each context c_i. As the probability $\Pr[Z_t = c_i]$ is fixed for a given time instant t and state c_i, the weights and the emission probabilities influence the final utility value. Subject to the constraint that a δ-privacy preserving is guaranteed, the simulations show that the larger the weight of a context $c_i$is set, the greater the number of original context $c_i$is released and the less the number of original context $c_i$is altered.

3. Data Storage and Retrieval in cloud

System enables a trigger strategy to the destruction of sensitive data. In order to protect the data we provide a backup in cloud storage for privacy preserving purposes, sensitive data and images are stored and retrieved using Elliptic Curve Cryptographic(ECC) algorithm.

The Firebase storage constitutes a unique pattern of data storage where the digital data is saved in logical pools, the physical storage covers manifold servers and at times locations with the physical scenario being classically owned and administered by a hosting company. The related Firebase storage providers are entrusted with the task of preserving the data for the sake of availability and accessibility by the genuine client and maintaining the physical scenario safe and effectively functional.

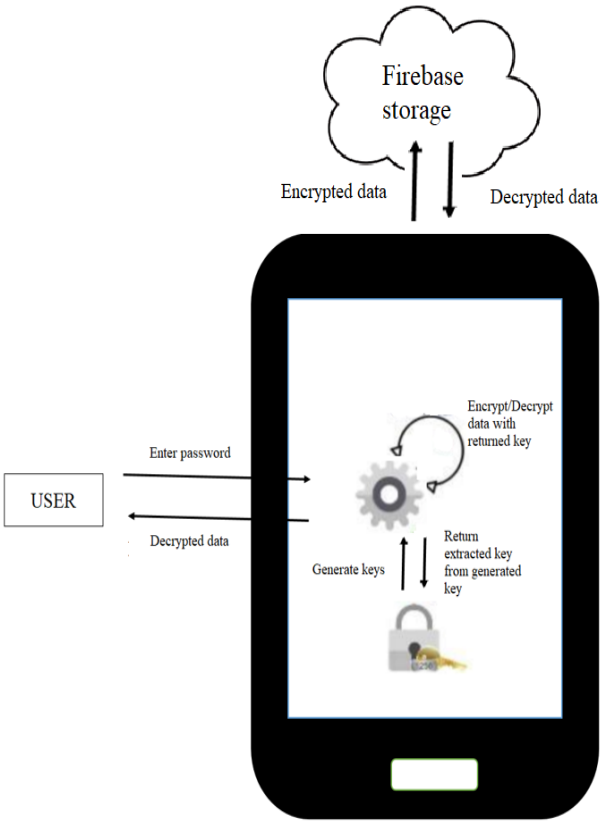

Fig.3 File Upload and Download using Elliptic Curve CryptographicAlgorithm

As Fig.3depicts the process flow of secure storage. The steps followed are illustrated below:

1) Application prompts the end user for the password.

2) End user provides the application with the password for performing cryptographic operations.

3) Application requests the key generation engine for the encryption key.

4) Key generation engine.

- Generates the master key with the user provided password.
- Extracts the content protection key with the generated master key.
- Send the extracted key to the application for performing encryption/decryption.

5) Application performs encryption/decryption of user data with the extracted key.

An Elliptic Curve Cryptographic (ECC) is exploited for the file encryption by creating a personal and public key of encryption in our suggested file. The personal and public keys are produced by the ECC method makes the updated input file more safe as well the produced keys are vigorous. Shorter keys reduce storage space for keys and faster computation speed which makes ECC suitable for constrained applications where computational power and bandwidth is limited.

Key Generation by ECC: Elliptic Curve Cryptographic (ECC) is as well-known as public key cryptography, which normally has a pair of keys, a public key and a private key and a set of actions associated with the keys to complete the cryptographic operations. The most important advantage of ECC is the small key size. The operations of elliptic curve cryptography are explained over two predetermined fields: Prime field and Binary field. For cryptographic operations, the suitable field is selected with finitely massive number of points. The prime field operations choose a prime number and finitely large numbers of basic points are produced on the elliptic curve, such that the generated points are between 0 to Z. Consequently, we randomly pick one basic point Pr (R1,

R2) for cryptographic operations and this point pleases the equation of the elliptic curve on a prime field, which is explained as

$V^2 \bmod P_{rm} = u^3 + \alpha u + \beta \bmod P_{rm}$--- (4)

α and β are the parameters that labelling the curve and u and v are the coordinate values of the generated points bp.

In order to randomly pick one basic point pr to carry out the cryptography, it is necessary to select a private key pv_{ky}, which arbitrarily select integers less than pv_{ky} and produce a public key $pu_{ky} = pv_{ky} * pr$. At this time, every updated file have detached private key pv_{ky} and public key pu_{ky}. The private and public values are inserted and that decimal value is changed into the binary value. Next least important bit is selected, which DataStream is employed for the encryption of the updated motion parameters.

Pixel grouping into a single integer: Images are made up of pixels. If cryptographic operation is performed on every single pixel it will take more time as the number of pixels present is very large. So, it will be a good option to group the pixels together. The number of pixels to be group depends on the Elliptic Curve parameters used. The larger the parameter of the elliptic curve, the more pixel can be grouped. For example a 512 bit ECC parameter can group upto 63 pixels together. To get the number of pixels to be group, find the number of the list, of the base 256 digits in the integer 'p' minus 1. To convert the group of pixels into a big single integer we have used a function of Mathematica called FromDigits [list of pixels, b] which take a list of pixels and convert it to base b. We add random 1 or 2 to each pixel to avoid error caused while using FromDigits function of Mathematica, in case, the first pixel value of the group is 0 and also to provide low correlated pixel value for the cipher image generated with same pixel value plain image. Pixel value of image in byte form will range from 0 to 255. So the maximum possible pixel value of the image will be 257 including the 2 we added. So, we will use base value 'b' as 258.

Getting the group of pixels from the big integer: After the ECC operation the coordinate value will all be in the range of the bit size chosen for the ECC operation. To generate the cipher image from these coordinates we need to bring it down to 0 to 255 range. We performed using the IntegerDigits [big integer value, 256] function in Mathematica. It takes as input the big integer values in the range of the size chosen for ECC operation and with base 256, the output will be a list of values ranging from 0 to 255. The two function, FromDigits [ ] and IntegerDigits [ ] are inverse of each other so the pixels value are preserved during the operation

V. PERFORMANCE ANALYSIS

The average fraction of released and suppressed states of sensitive and normal data are shown in Fig.4. Although all sensitive states are suppressed, an adversary who knows the Markov chain of states can infer near 20 % sensitive states from the suppressed ones. This is because the temporal correlation among states indicates enough information for an adversary, and makes the posterior belief to exceed with prior belief by more than the privacy parameter δ.

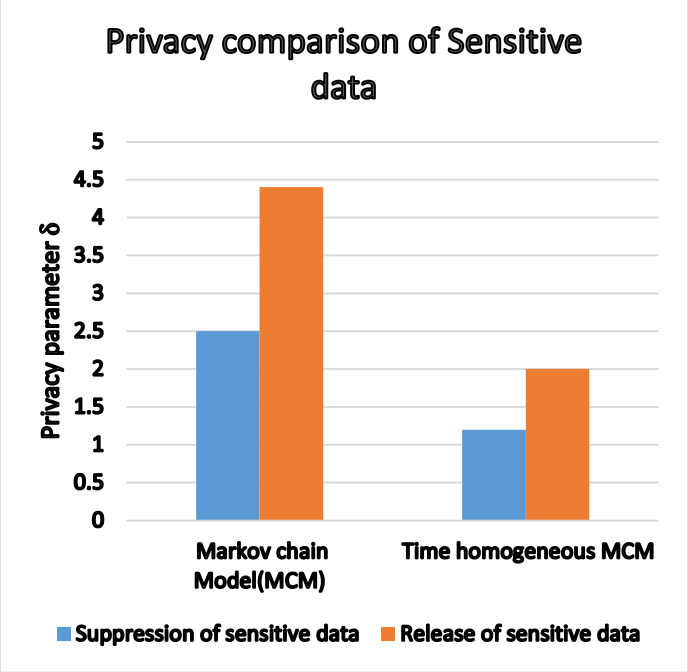

Fig.4 Privacy Comparison of Sensitive data

The time required to upload and download a file is reduced in the proposed system which is clearly depicted in Fig. 5 and Fig. 6 respectively.

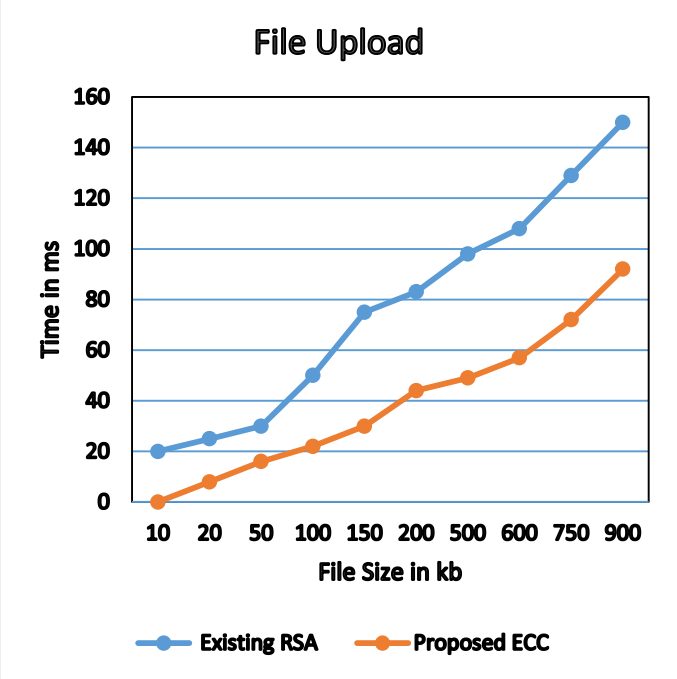

Fig.5File upload time

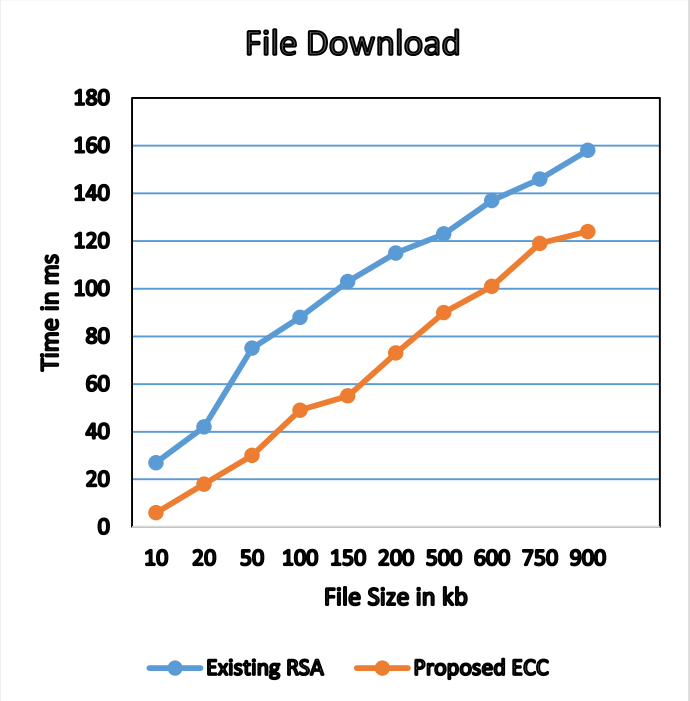

Fig.6File download time

CONCLUSION

The proposed system generates fake data to intruders using time homogeneous Markov Chain model and it decides whether to release the real context or a fake one. Since a real context of a user may be disguised as any of the contexts under the deception policy, an adversary has a great difficulty to infer the real context, leading to achieving greater utility than other policies such as hiding-sensitive policy. We also provides a trigger, it delete the sensitive data if the password is incorrect for more than 4 times which protect the sensitive data. Using Time homogeneous Markov chain model not only sensitive data is suppressed and released but also normal data.The system provide a backup in cloud storage for privacy preserving purposes, sensitive data and images are stored and retrieved using Elliptic Curve Cryptographic (ECC) algorithm. However, even if proposed system provides the comprehensive protection still leakage of sensitive data is possible.

REFERENCES

1. Shuangxi Hong, Chuanchang Liu, Bingfei Ren, Yuze Huang, and Junliang Chen, “Personal Privacy Protection Framework Based on Hidden Technology for Smartphones”, IEEE Transactions, Vol. 5, May 17, 2017. (BASE PAPER)
2. Mazhar Ali, RevathiDhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya, “SeDaSC: Secure Data Sharing in Clouds”, IEEE Systems Journal Vol. 11, No. 2, June 2017.
3. A. Skillen and M. Mannan, “Mobi_age: Deniable storage encryption for mobile devices,” IEEE Transactions on Dependable and Secure Computing, Vol. 11, No. 3, May/Jun. 2014.
4. Chang, Z. Wang, B. Chen, and F. Zhang, “MobiPluto: File system friendly deniable storage for mobile devices”, in 31stAnnual Computer Security Applications Conference. USA, 2015.

5. John Bethencourt, Amit Sahai, Brent Waters, “Ciphertext-Policy Attribute-Based Encryption”, IEEE Symposium on Security and Privacy,2007.
6. Michaela Götz, SumanNath, Johannes Gehrke, “MaskIt: Privately Releasing User Context Streams for Personalized Mobile Applications”, in ACM SIGMOD International Conference on Management of Data (SIGMOD) USA, May 2012.
7. Wei Wang, Qian Zhang, “A Stochastic Game for Privacy Preserving Context Sensing on Mobile Phone”, IEEE Conference on Computer Communications (INFOCOM), 2014.
8. Wei Wang, Qian Zhang, “Privacy Preservation for Context Sensing on Smartphone”, IEEE/ACM Transactions on Networking, 2016.
9. B. Shebaro, O. Oluwatimi, and E. Bertino, “Context-based access control systems for mobile devices”,IEEE Transactions on dependable and Secure computing2015.
10. A. N. Khan, M. M. Kiah, S. A. Madani, M. Ali, and S. Shamshir-band, “Incremental proxy re-encryption scheme for mobile cloud computing environment,” The Journal of Super Computing Springer. 2014.
11. W. Encket al., “TaintDroid: An information flow tracking system for real-time privacy monitoring on smartphones”,Communications of the ACM, 2014.
12. B. Gedik and L. Liu, “Location privacy in mobile systems: A personalized anonymization model”, in Proceedings of 25th International Conference on Computer Communications, Columbus, USA, Jun. 2005.
13. L. Wei, H. Zhu, Z. Cao, Y. Chen, and A. V. Vasilakos, “Security and privacy for storage and computation in cloud computing”,Information of Sciences, Feb. 2014.
14. X. Liang, K. Zhang, X. Shen, and X. Lin, “Security and privacy in mobile social networks: Challenges and solutions”,IEEE Wireless Communications., Feb. 2014.
15. https://developer.android.com/studio/index.html.